Formulário para Solicitação de Autorização de Dispensa de Licitação

Unidade:
DTI - CASI

Objeto:
A presente licitação tem por objeto a contratação de serviços realização de PENTEST (teste de invasão) na abordagem Blackbox na aplicação Voto Eletrônico.

Enquadramento do Objeto:
Prestação de Serviços

Indicação da Necessidade para a Contratação:
Atender demanda institucional visando atender a necessidade de realizar testes de vulnerabilidade digital na aplicação Voto Digital,.

Fundamentação Legal - Lei Nº 9.433/05, art. 59, inciso

I Obras e serviços de engenharia, desde que não se refiram a uma mesma obra/serviço ou de mesma natureza e local que possa ser realizado conjunta e concomitantemente.
Não

II Contratação de serviços e compras, desde que não se refiram a parcelas de um mesmo serviço/compra de maior ulto que possa ser realizada de uma vez só.
Sim

Outros (especificar):
-

PROPOSTAS APRESENTADAS

Proposta 1:

1-Item:
Pentest Voto Digital

1-Fornecedor (Nome / Razão Social):
Ibliss Digital Security

1-Valor Total (R$):
12.000,00

Proposta 2:

2-Item:
Pentest Voto Digital

2-Fornecedor (Nome / Razão Social):
Stefanini Rafael Segurança e Defesa S.A

2-Valor Total (R$):
8.202,67

Proposta 3:

3-Item:
Pentest Voto Digital

3-Fornecedor (Nome / Razão Social):
VIVO Empresas

3-Valor Total (R$):
41.186,85

FORNECEDOR(es) SELECIONADO(s)

1-Fornecedor (Nome / Razão Social):
Stefanini Rafael Segurança e Defesa S.A

1-Endereço:
Avenida Eusebio Matoso 1375,8º andar, sala 801,802 - SP-SP, CEP:05423-905

1-CPF/CNPJ:
246914880001-09

1-Valor (R$):
8.202,67

2-Fornecedor (Nome / Razão Social):
-

2-Endereço:
-

2-CPF/CNPJ:
-

2-Valor (R$):
-

3-Fornecedor (Nome / Razão Social):
-

3-Endereço:
-

3-CPF/CNPJ:
-

3-Valor (R$):
-

Documento assinado eletronicamente por **laçanã Lima de Jesus Carneiro** em 29/07/2021, às 10:26, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.sistemas.mpba.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0163778** e o código CRC **D38F937A**.

1. OBJETO		
1.1 DEFINIÇÃO DO OBJETO	**Especificação do Objeto** Contratação de serviços realização de PENTEST (teste de invasão) na abordagem Blackbox na aplicação Voto Eletrônico. **Observação**: Detalhamento dos itens que compõem o objeto constam na tabela 1 do ANEXO I (indicado ao final do documento).	
1.2 FORMA DE CONTRATAÇÃO ESCOLHER UMA DAS TRÊS OPÇÕES ***(Marcar com X)***:	**(x)**	**A) PRESTAÇÃO DE SERVIÇOS IMEDIATA (PONTUAL/POR ESCOPO)**
	( )	**B) PRESTAÇÃO DE SERVIÇOS PARCELADA**
	( )	**C) PRESTAÇÃO DE SERVIÇOS SOB DEMANDA**
	( )	**D) OUTROS:**
1.3 JUSTIFICATIVA: **NECESSIDADE DA CONTRATAÇÃO**	O Ministério Público do Estado da Bahia (MPBA) encontra-se em plena transformação digital, passando por mudança de cultura e adoção de novos procedimentos que estão sendo alicerçados pela tecnologia da informação. Neste contexto, a Alta Administração da instituição decidiu pela realização das eleições internas através de sistema informatizado de votação denominado VOTO DIGITAL. Originalmente cedido pelo Ministério Público do Estado de São Paulo com o nome VOTO ELETRÔNICO, o sistema foi instalado e configurado no ambiente tecnológico do MPBA e posteriormente adaptado para funcionar de acordo com as regras estabelecidas pelos seus gestores, passando a ser chamado de VOTO DIGITAL. De forma inovadora, será possibilitado que os membros do MPBA possam votar a partir de computadores ou dispositivos móveis conectados à *internet*, mediante dupla autenticação e outros requisitos de segurança. É sabido que os processos eleitorais são sujeitos a críticas ainda mais quando envolvem tecnologia da informação e comunicação. Objetivando garantir a máxima segurança da informação possível no sistema VOTO DIGITAL, o MPBA vem realizando ações tecnológicas e procedimentais visando garantir a lisura e transparência de todo o processo eleitoral assim como das ferramentas tecnológicas envolvidas.	

	O MPBA entende que a realização de um Teste de Intrusão - PENTEST -, conjunto de testes visando detectar falhas e/ou vulnerabilidades da referida aplicação e na infraestrutura que a suporta, utilizando técnicas dos Hackers éticos - especialistas em segurança da informação, irá possibilitar o conhecimento maior sobre a aplicação e sua infra com o intuito de ter um ambiente o mais seguro possível, atendendo aos princípios basilares da segurança da informação - Integridade, Confiabilidade e Disponibilidade. A presente contratação visa a realização de uma análise independente e externa a área de TI do MPBA com o objetivo de eliminar eventuais vulnerabilidades do sistema VOTO DIGITAL contribuindo para que o mesmo seja executado de maneira segura.
1.4 JUSTIFICATIVA: **QUANTITATIVO(S) DEFINIDO(S)**	Será realizado um Pentest completo – testes, mitigações de possíveis vulnerabilidades encontrada, reteste para assegurar que as vulnerabilidades foram devidamente mitigadas, durante o prazo da contratação para a aplicação Voto Eletrônico. Assim se tem de forma inequívoca que os requisitos de proteção a aplicação, na esfera dos testes de intrusão, foram atendidos.

1.5 INDICAÇÃO DE MODELO E/OU MARCA OBRIGATÓRIOS ESCOLHER UMA OPÇÃO* ***(Marcar com X)***:	**( )** SIM	**(x)** NÃO
	1.5.1 INDICAÇÃO DO(S) ITEM(NS) E DO MODELO/MARCA - Em caso positivo:	
	1.5.2 JUSTIFICATIVA PARA CADA ITEM - Em caso positivo:	

2. FUNDAMENTO LEGAL

2.1 INDICAÇÃO DO DISPOSITIVO LEGAL EM QUE SE ENQUADRA A HIPÓTESE DE CONTRATAÇÃO ESCOLHER UMA OPÇÃO* ***(Marcar com X)***:	**( )**	**A) Artigo 59, I da Lei Estadual/BA nº 9.433/2005** - para obras e serviços de engenharia de valor não excedente a 10% (dez por cento) do limite previsto para modalidade de convite, desde que não se refiram a parcelas de uma mesma obra ou serviço, ou ainda para obras e serviços da mesma natureza e no mesmo local que possam ser realizadas conjunta e concomitantemente;
	(x)	**B) Artigo 59, II da Lei Estadual/BA nº 9.433/2005** - para serviços e compras de valor até 10% (dez por cento) do limite previsto para compras e serviços que não sejam de engenharia, na modalidade de convite, e para alienações, nos casos previstos nesta Lei, desde que não se refiram a parcelas de um mesmo serviço, compra ou alienação de maior vulto que possa ser realizada de uma só vez;

	( )	C) **OUTROS**

3. REGRAS DE CONTRATAÇÃO

3.1 REGRAS DE FORMALIZAÇÃO CONTRATUAL	**3.1.1 HAVERÁ CELEBRAÇÃO DE CONTRATO** **(x) A SIM** **( ) B NÃO (FORMALIZAÇÃO SE DARÁ APENAS COM A EMISSÃO DE EMPENHO)**
3.2 REGRAS DE EXECUÇÃO CONTRATUAL	**3.2.1 REGIME DE EXECUÇÃO:** **( ) Empreitada por preço** **(x) Empreitada por preço global** **( ) Outro:** **3.2.2 PRAZO PARA RETIRADA DA NOTA DE EMPENHO:** ➢ 5 dias **( )** Úteis **(x)** Corridos. ➢ Contados da convocação pelo Ministério Público, a ser formalizada preferencialmente por e-mail. **3.2.3 PRAZOS DE EXECUÇÃO** ➢ 30 dias **( )** Úteis **(x)** Corridos ➢ O prazo será contado da data do recebimento, pelo Fornecedor, da Nota de Empenho, acompanhada da autorização de fornecimento e, se for o caso, do instrumento contratual.

3.2.4 ADMISSIBILIDADE DE PRORROGAÇÃO DO PRAZO DE EXECUÇÃO

( )	**A) NÃO**
(x)	**B) SIM.** Neste caso, somente será admissível o pedido formalizado pelo fornecedor antes do termo final do prazo de entrega consignado, mediante justificativa - e respectiva comprovação - de fato superveniente, aceito pela Instituição. ➢ Por até 30 dias **(x)** Úteis **( )** Corridos

3.2.5 LOCAL DE EXECUÇÃO DOS SERVIÇOS: Ministério Público do Estado da Bahia - Sede Principal: 5ª Avenida, n° 750, do CAB - Salvador, BA - Brasil - CEP: 41.745-004

3.2 REGRAS DE EXECUÇÃO CONTRATUAL		
		3.2.6 REGRAS ESPECIAIS PARA EXECUÇÃO: ➢ Execução deve ser agendada - ESCOLHER UMA OPÇÃO ***(Marcar com X)***: **( )** A) NÃO **(x)** B) SIM ➢ Unidade responsável: Diretoria de Tecnologia da Informação ➢ Telefone e e-mail para contato e/ou agendamento: (71) 3103-0214 e casi@mpba.mp.br ➢ Dias para realização da entrega dos serviços: Durante o mês de outubro de 2021 ➢ Horários para execução: Pela natureza do serviço serão acertados a posteriori quando da execução. ➢ Condições especiais adicionais: Não há
3.3 GARANTIA DO OBJETO ESCOLHER UMA OPÇÃO * ***(Marcar com X)***:	**(x)**	**A) SEM EXIGÊNCIA DE GARANTIA**
	( )	**B) COM EXIGÊNCIA DE GARANTIA** - Regras: ➢ **EXECUTOR DA GARANTIA** - ESCOLHER UMA OPÇÃO ***(Marcar com X)***: **( )** A) CONTRATADA (Regra geral) **( )** B) FABRICANTE (Exceção) ➢ Justificar a exigência de garantia do fabricante (Em caso positivo): ➢ **DURAÇÃO** - ESCOLHER UMA OPÇÃO ***(Marcar com X)***: **( )** A) 01 ANO **( )** B) 90 DIAS (GARANTIA LEGAL) **( )** C) OUTRO. Especificar:

		➢ **PRAZO MÁXIMO PARA RESOLUÇÃO DO CHAMADO, contado a partir da abertura pelo MPBA** - ESCOLHER UMA OPÇÃO ***(Marcar com X)***: **( )** A) _____ HORAS **( )** Úteis **( )** Corridas **( )** B) _____ DIAS **( )** Úteis **( )** Corridos ➢ **NECESSIDADE DE ASSISTÊNCIA TÉCNICA** - ESCOLHER UMA OPÇÃO ***(Marcar com X)***: **( )** A) SIM **(x)** B) NÃO ➢ **FORMA DE EXECUÇÃO DA ASSISTÊNCIA TÉCNICA** (Se resposta positiva acima) - ESCOLHER UMA OPÇÃO ***(Marcar com X)***: **( )** A) Assistência sediada na zona urbana ou metropolitana de Salvador **( )** B) Assistência sediada em local a critério do fornecedor (regra geral) **( )** C) *On site*, isto é assistência prestada diretamente na sede do MPBA (exceção). Regras: ○ Os chamados para Assistência Técnica deverão ser atendidos no prazo máximo de _____ (_____) horas, contadas da notificação pelo MPBA; ○ O Fornecedor ou Fabricante (conforme regra de "Executor" acima indicada) arcará com todas as despesas decorrentes da reparação e/ou substituição de bens, a incluir o deslocamento de seus técnicos aos locais em que aqueles estiverem, bem como pelo transporte para sua oficina, se necessário; **( )** D) Outra. Especificar: ➢ **DEMAIS REGRAMENTOS**:
3.4 CONDIÇÕES E RESPONSÁVEIS PELO RECEBIMENTO *	**3.4.1 PRAZO PARA RECEBIMENTO PROVISÓRIO:** 5 dias **( )** Úteis **(X)** Corridos	
	3.4.2 PRAZO PARA RECEBIMENTO DEFINITIVO: 10 dias **( )** Úteis **(X)** Corridos	
	3.4.3 UNIDADE RESPONSÁVEL PELO RECEBIMENTO: Diretoria de Tecnologia da Informação	
	3.4.4 PRAZO PARA ADEQUAÇÃO OU REFAZIMENTO DE SERVIÇO(S) REJEITADO(S) - ESCOLHER UMA OPÇÃO ***(Marcar com X)***: **(X)** A) NÃO SE APLICA	

	( ) B) PRAZO: ( ) _____ HORAS ( ) Úteis ( ) Corridas ( ) _____ DIAS ( ) Úteis ( ) Corridos	
	DEMAIS REGRAMENTOS: 3.4.5 O recebimento dos serviços ocorrerá mediante conferência destes, confrontando com as especificações contidas no Termo de Referência e Contrato (inclusive anexos) e na proposta de preços, bem com as quantidades determinadas na Ordem de serviços/Nota de Empenho. 3.4.6 O recebimento dado pelo Ministério Público do Estado da Bahia em fatura (ou documento afim) apresentada por transportadora a serviço do fornecedor não será considerado para fins de recebimento provisório/definitivo; 3.4.7 O recebimento definitivo do objeto deste contrato só será concretizado depois de adotados, pelo Ministério Público do Estado da Bahia, todos os procedimentos contidos nos Ato Normativos internos relativos ao tema, respeitadas as exigências contidas do art. 161 da Lei Estadual- BA nº 9.433/2005; 3.4.8 O aceite ou aprovação do objeto pelo Ministério Público do Estado da Bahia não exclui a responsabilidade do fornecedor por vícios, defeitos ou disparidades com as especificações estabelecidas neste Contrato e no processo de Dispensa Licitação que o originou, verificadas posteriormente, garantindo-se ao Ministério Público do Estado da Bahia, inclusive, as faculdades previstas na Lei Federal n.º 8.078/90 – Código de Defesa do Consumidor.	
3.5 POSSIBILIDADE OU NÃO DE SUBCONTRATAÇÃO ESCOLHER UMA OPÇÃO *(Marcar com X)*:	**(X)**	**A) VEDADA A SUBCONTRATAÇÃO**
	( )	**B) ADMITIDA A SUBCONTRATAÇÃO DE SERVIÇOS ACESSÓRIOS.** ➢ Indicar parcela(s) subcontratável(eis): ➢ Indicar regras/condições para subcontratação:
3.6 CONDIÇÕES DE PAGAMENTO	**3.6.1 PERIODICIDADE DE PAGAMENTO** - ESCOLHER UMA OPÇÃO *(Marcar com X)*:	
	(X)	**A) PAGAMENTO INTEGRAL, AO FINAL DA EXCUÇÃO E RECEBIMENTO DOS SERVIÇOS**
	( )	**B) CADA PEDIDO (E CONSEQUENTE EMPENHO EMITIDO) SERÁ PAGO INTEGRALMENTE, EM PARCELA ÚNICA**

( )	**C) PAGAMENTO PARCELADO:** ➢ Quantidade de parcelas: ➢ Definição dos montantes das parcelas (Por quantidades ou percentuais, conforme regime de execução e regramentos eventualmente definidos no anexo mencionado no item 1.2.):
( )	**C) PAGAMENTO MENSAL**
( )	**D) OUTRA:**

3.6.2 CONDIÇÕES ESPECIAIS PARA EFETIVAÇÃO DO PAGAMENTO - ESCOLHER UMA OPÇÃO ***(Marcar com X)***:

(X)	**A) NÃO SE APLICA**
( )	**B) CONDIÇÕES ESPECIAIS. Especificar:**

3.6.3 DEMAIS REGRAS:

3.6.3.1 O pagamento será processado mediante apresentação, pela contratada, de nota fiscal e certidões cabíveis - documentação esta que deverá estar devidamente acompanhada do ACEITE pelo Ministério Público do Estado da Bahia, e se concluirá no prazo de 08 (oito) dias úteis a contar da data de apresentação da documentação, desde que não haja pendência a ser regularizada;

3.6.3.2 Verificando-se qualquer pendência impeditiva do pagamento, será considerada como data de apresentação da documentação aquela na qual foi realizada a respectiva regularização;

3.6.3.3 As notas fiscais deverão discriminar os tributos, com respectivos valores, alíquotas e bases de cálculo, que tenham como fato gerador o objeto contratado;

3.6.3.4 O Ministério Público do Estado da Bahia realizará a retenção de impostos ou outras obrigações de natureza tributária, na hipótese de figurar como substituto tributário, de acordo com a legislação vigente;

3.6.3.5 Os pagamentos serão efetuados através de ordem bancária, para crédito em conta corrente e agência indicadas pela empresa contratada, preferencialmente em banco de movimentação oficial de recursos do Estado da Bahia;

3.6.3.6 A atualização monetária dos pagamentos devidos pelo Ministério Público do Estado da Bahia, em caso de mora, será calculada considerando a data do vencimento da obrigação e do seu efetivo pagamento, de acordo com a variação do INPC do IBGE pro rata tempore, observado, sempre, o disposto no item 3.6.3.2.

3.7 POSSIBILIDADE OU NÃO DE REAJUSTAMENTO, COM INDICAÇÃO DE ÍNDICE OFICIAL ESCOLHER UMA OPÇÃO * ***(Marcar com X):***	**(X)**	**A) PREÇOS IRREAJUSTÁVEIS**
	( )	**B) PREÇOS PASSÍVEIS DE REAJUSTAMENTO.** Regras: ➢ Índice oficial para o cálculo da variação de preços - ESCOLHER UMA OPÇÃO ***(Marcar com X)***: **( )** A) INPC/IBGE **( )** B) OUTRO. Indicar: ➢ A eventual concessão de reajustamento fica condicionada à apresentação de requerimento formal pelo Fornecedor, após o transcurso do prazo de 12 (doze) meses, contados da data da apresentação da proposta; ➢ Na hipótese de reajustamento, adotar-se-á como referencial o acumulado de 12 (doze) meses, sendo o termo inicial o mês de apresentação da proposta e termo final o mês que antecede a data de aniversário. ➢ Serão objeto de reajuste apenas os valores relativos a pedidos de serviços formalizados após o decurso do prazo de 12 (doze) meses, contados da apresentação da proposta;
3.8 DEFINIÇÃO DE VIGÊNCIAS *	**3.8.1 DEFINIÇÃO DE VIGÊNCIA DA CONTRATAÇÃO** - ESCOLHER UMA OPÇÃO ***(Marcar com X):***	
	( )	**A) CONTRATAÇÕES SEM INSTRUMENTO FORMAL DE CONTRATO** ➢ ESCOLHER UMA OPÇÃO ***(Marcar com X):*** **( ) Opção 1:** _____ meses , contados do recebimento do empenho pelo fornecedor **( ) Opção 2:** _____ dias, contados do recebimento do empenho pelo fornecedor
	(X)	**B) CONTRATAÇÕES COM INSTRUMENTO FORMAL DE CONTRATO** ➢ ESCOLHER UMA OPÇÃO ***(Marcar com X):*** **( ) Opção 1:** _____ meses, contados a partir de(a) - ESCOLHER UMA OPÇÃO ***(Marcar com X):*** **( )** A) Data certa: ____ de _____ de _____ **( )** B) Da data da publicação do resumo do contrato no Diário da Justiça Eletrônico

		(x) Opção 2: 90 dias, contados a partir de(a) - ESCOLHER UMA OPÇÃO *(Marcar com X):* **( )** A) Data certa: ____ de _____ de _____ **(x)** B) Da data da publicação do resumo do contrato no Diário da Justiça Eletrônico ➢ Justificar vigência superior a 12 (doze) meses (se for o caso):
	3.8.2 POSSIBILIDADE DE PRORROGAÇÃO DE PRAZO DE VIGÊNCIA - ESCOLHER UMA OPÇÃO *(Marcar com X):*	
	( )	**A) NÃO**
	(x)	**B) SIM.** Justificativa: Diante da eventual necessidade de dilação da execução contratual faz-se necessário prever a possibilidade de prorrogação do prazo de vigência.
3.9 OBRIGAÇÕES DA CONTRATADA*	**OBRIGAÇÕES GERAIS** 3.9.1 Executar o objeto contratual de acordo com os prazos e as especificações técnicas constantes no instrumento convocatório e seus anexos, no local determinado, nos dias e nos turnos e horários de expediente do MPBA, não podendo eximir-se da obrigação, ainda que parcialmente, sob a alegação de falhas, defeitos ou falta de pessoal, materiais e/ou peças; 3.9.2 Adotar as providências legais e/ou contratuais cabíveis, nas ocorrências de danos no decurso do uso normal do produto durante o prazo de garantia e por defeitos de fabricação; 3.9.3 Promover, às suas expensas e sob sua responsabilidade, a adequada embalagem, transporte e entrega do(s) bem(ns); 3.9.4 Prestar diretamente o objeto contratado, não o transferindo a outrem, no todo ou em parte, ressalvando-se apenas os casos de cisão, fusão ou incorporação da empresa contratada, desde que não impeçam os compromissos assumidos para com o **MPBA**, observando-se, ainda, eventuais restrições à subcontratação definidas neste instrumento; 3.9.5 Manter durante toda a execução da contratação, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas no procedimento de contra; 3.9.6 Providenciar e manter atualizadas todas as licenças e alvarás junto às repartições competentes que, porventura, sejam necessários à execução da contratação; 3.9.7 Responsabilizar-se pelo cumprimento das exigências previstas na legislação profissional específica e pelos encargos fiscais e comerciais resultantes da execução da contratação;	

3.9.7.1 A eventual retenção de tributos pelo **MPBA** não implicará na responsabilização deste, em hipótese alguma, por quaisquer penalidades ou gravames futuros, decorrentes de inadimplemento(s) de tributos pela empresa contratada;

3.9.8 Emitir notas fiscais/faturas de acordo com a legislação e com este documento, contendo descrição dos serviços, indicação de quantidades, preços unitários e valor total;

3.9.9 Arcar, quando da execução do objeto contratado, com todo e qualquer dano ou prejuízo, independentemente da natureza, causado ao **MPBA** e/ou a terceiros, ainda que por sua culpa, em consequência de erros, imperícia própria ou de auxiliares que estejam sob sua responsabilidade, bem como ressarcir ao **MPBA** todos os custos decorrentes de indevida paralisação ou interrupção dos serviços contratados;

3.9.10 Não introduzir, seja a que título for, nenhuma modificação na especificação do objeto contratado ou das eventuais normas técnicas a serem seguidas, sem o consentimento prévio, e por escrito, do **MPBA**;

3.9.11 Atender, nos prazos consignados neste instrumento e/ou pelo **MPBA**, às recusas ou determinações de desfazimento/refazimento fornecimentos e/ou serviços acessórios que não estejam sendo ou não tenham sido executados de acordo com as Normas Técnicas e/ou em conformidade com as condições do Edital (e anexos) constante no processo que o originou, providenciando sua imediata correção ou realização, sem ônus para o **MPBA**;

3.9.12 Permitir e oferecer condições para a mais ampla e completa fiscalização durante a vigência da contratação, fornecendo informações, propiciando o acesso à documentação pertinente e à execução contratual, e atendendo às observações e exigências apresentadas pela fiscalização;

3.9.13 Comunicar formalmente ao **MPBA** qualquer anormalidade que interfira no bom andamento da execução da contratação;

3.9.14 Manter sob sua exclusiva responsabilidade toda a supervisão e direção da eventual mão de obra necessária à execução completa e eficiente da contratação;

3.9.15 Prestar todos os esclarecimentos que forem solicitados pelo **MPBA**.

OBRIGAÇÕES ESPECÍFICAS (DEFINIDAS EM RAZÃO DO OBJETO CONTRATADO):

( )	**A) NÃO EXISTEM OBRIGAÇÕES ESPECÍFICAS**, sendo aplicáveis somente os regramentos gerais definidos no subitem anterior.
	B) OBRIGAÇÕES ESPECÍFICAS. Indicar:
(X)	**1. SIGILO E INVIOLABILIDADE**
	1.1. A CONTRATADA compromete-se a manter em caráter confidencial as informações abaixo mencionadas, mesmo após a eventual rescisão do contrato:

		1.1.1. Política de segurança adotada pelo CONTRATANTE e configurações de hardware e software decorrentes; 1.1.2. Processo de instalação, configuração e customizações de produtos, ferramentas e equipamentos e atendimento aos itens de segurança, constantes do Edital de licitação; 1.1.3. Processo de implantação no ambiente do CONTRATANTE, de mecanismos de criptografia e autenticação utilizados; 1.1.4. Recomendações e implementações decorrentes do processo de consultoria; 1.1.5. Quaisquer dados que a CONTRATADA venha a ter conhecimento em decorrência da presente contratação, pertinentes a hardware, serviços e sistemas aplicativos do CONTRATANTE, cujo conhecimento por terceiros exponha o ambiente a riscos de invasão ou resulte na vulnerabilidade do mesmo. 1.1.6. Não fazer uso das informações prestadas pela CONTRATANTE que não seja em absoluto cumprimento ao contrato em questão. 1.1.7. A quebra da confidencialidade ou sigilo de informações obtidas na prestação de serviços ensejará multa, responsabilidade criminal na forma da lei, sem prejuízo de outras providências nas demais esferas. A CONTRATADA obriga-se a tomar as providências necessárias para assegurar que as informações confidenciais não sejam divulgadas por seus empregados ou agentes. 1.1.8. Assinar o Termo de Confidencialidade constante do anexo deste instrumento, no qual se comprometerá a guardar os dados e as informações fornecidas, geradas e/ou de propriedade do MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA, de forma confidencial e sigilosa, vedada qualquer forma de divulgação, reprodução e/ou cessão.
3.10 OBRIGAÇÕES DO CONTRATANTE*		**OBRIGAÇÕES GERAIS** 3.10.1 Fornecer, no prazo de até 10 (dez) dias a contar do início da vigência da contratação, as informações necessárias para que a empresa contratada possa executar plenamente o objeto contratado; 3.10.2 Realizar os pagamentos devidos pela execução do contrato, nos termos e condições previstos neste documento; 3.10.3 Permitir o eventual acesso dos empregados autorizados da empresa contratada às instalações físicas do **MPBA**, nos locais e na forma que se façam necessários para a execução contratual; 3.10.4 Acompanhar e fiscalizar o fiel cumprimento dos prazos e das condições da contratação, notificando a empresa contratada, por escrito, sobre imperfeições, falhas ou irregularidades constatadas na execução do objeto, para que sejam adotadas as medidas corretivas necessárias; 3.10.5 Fornecer à empresa contratada, mediante solicitação, atestado de capacidade técnica, quando o fornecimento do objeto atender satisfatoriamente os prazos de entrega, qualidade e demais condições previstas em edital e seus anexos.

		OBRIGAÇÕES ESPECÍFICAS (DEFINIDAS EM RAZÃO DO OBJETO CONTRATADO):
	(X)	**A) NÃO EXISTEM OBRIGAÇÕES ESPECÍFICAS,** sendo aplicáveis somente os regramentos gerai definidos no subitem anterior.
	( )	**B) OBRIGAÇÕES ESPECÍFICAS.** Indicar:
3.11 INDICAÇÃO SOBRE A NECESSIDADE DE GARANTIA CONTRATUAL, COM PERCENTUAL ESCOLHER UMA OPÇÃO ***(Marcar com X):***	**( )**	**A) NÃO SE APLICA (CONTRATAÇÕES SEM FORMALIZAÇÃO DE CONTRATO)**
	(X)	**B) NÃO SERÁ EXIGIDA GARANTIA CONTRATUAL**
	( )	**C) SERÁ EXIGIDA GARANTIA CONTRATUAL.** Regras: ➢ Percentual exigido: **( )** 5% (cinco por cento) **OU** **( )** Outro. Indicar: _____ % (_____ por cento) ➢ Prazo para apresentação: _____ dias após assinatura do contrato.

ANEXO I – TABELA INDICATIVA DE ITENS

1. INDICAÇÃO DOS ITENS QUE COMPÕEM O OBJETO:

1.1 DETALHAMENTO DOS ITENS

Item	Descrição (Especificações técnicas)	Unidade de Fornecimento	Quantidade	Valor unitário	Valor total por item
1	Pentest (Teste De Intrusão)	UND	1	R$ 8.202,67	R$ 8.202,67
Valor Total dos itens					R$ 8.202,67

ANEXO II – ESPECIFICAÇÕES TÉCNICAS DETALHADAS

2. Caraterísticas Gerais:

2.1. A atividade de Teste de Intrusão/Penetração (Pentest) deve compreender o teste de Invasão externa e tem como objetivo principal identificar, possíveis vulnerabilidades na aplicação WEB VOTO ELETRÔNICO da CONTRATANTE. Estes testes envolvem o uso de técnicas e ferramentas para tentar o acesso privilegiado aos ativos e informações da CONTRATANTE por meio de simulações controladas de ataques reais, sendo o ambiente da aplicação da CONTRATANTE avaliado em sua totalidade em busca de vulnerabilidades que possam permitir a obtenção de acesso não-autorizado, sendo que a modalidade de teste de intrusão/penetração a ser realizado será do tipo Black Box.

2.2. O teste Black Box parte da premissa que o profissional não tem informações sobre o sistema nem da estrutura da empresa e trata a aplicação como uma "caixa preta". Sendo mais difícil de ser aplicado, já que é preciso colher algumas informações para tentar explorar vulnerabilidades, mas em compensação, essa simulação fica mais próxima de um ataque real feito externamente por hackers.

2.3. A CONTRATADA deverá realizar testes de intrusão para identificação de vulnerabilidades por meio de simulações de invasão de serviços e infraestrutura (Teste de Invasão) a serem executadas externamente (através da Internet), com duração de até 30 (trinta) dias.

2.4. A CONTRATADA deverá elaborar "Relatório de Teste de Invasão" para cada teste realizado no período, apresentando todas as informações sobre o mesmo, contemplando no mínimo: objetivos, premissas e escopo do teste; metodologia de análise de vulnerabilidades; descrição das ações realizadas; vulnerabilidades encontradas; categorização e severidade das vulnerabilidades, recomendações e controles de segurança necessários para correção das vulnerabilidades; apresentação das evidências; referências e ferramentas utilizadas. Pelo período de 30 (trinta) dias, este "Relatório de Teste de Invasão" será o insumo para que a equipe técnica da CONTRATANTE possa realizar as mitigações necessárias visando sanar as vulnerabilidades o apontadas.

2.5. A Metodologia adotada pela CONTRATADA durante o Pentest deve incluir minimamente, quando pertinente, as seguintes vulnerabilidades:

2.5.1. Injeção de Código.
2.5.2. Quebra de Autenticação.
2.5.3. Exposição de Dados Sensíveis.
2.5.4. Entidades Externas de XML.
2.5.5. Quebra de Controle de Acesso.
2.5.6. Configuração Incorreta de Segurança.
2.5.7. Cross-Site Scripting (XSS).
2.5.8. Desserialização Insegura.
2.5.9. Utilização de Componentes com Vulnerabilidades Conhecidas.
2.5.10. Log e Monitoramento Ineficientes.

2.6. A CONTRATADA deverá minimamente compreender atividades que busquem encontrar vulnerabilidades em potencial, de eventual má configuração, de falhas em hardwares e softwares desconhecidos, de técnicas de contramedidas ou deficiências na infraestrutura ou sistemas da CONTRATANTE;

2.7. A CONTRATANTE deve criar um usuário interno para a CONTRATADA no ambiente da CONTRATANTE com todas suas ações logadas para documentação e atestar a integridade do trabalho realizado pela CONTRATADA.
2.8. O alvo do PENTEST (Teste de Invasão) será a aplicação aqui denominada VOTO ELETRÔNICO. Todas as fases dos PENTEST poderão ser acompanhadas e supervisionadas a qualquer momento pelo CONTRATANTE. Quaisquer atividades com suspeita de comprometimento de algum ambiente ou ativo, deverá a CONTRATADA ser reportada pelo CONTRATANTE;
2.9. Os serviços contratados deverão ser obrigatoriamente executados fora das dependências da CONTRATANTE.

2.10. O teste de penetração deverá incluir ,no mínimo, as seguintes técnicas de teste:
2.10.1. Ping sweep de intervalos de redes;
2.10.2. Verificação de portas de hosts de destino;
2.10.3. Verificação de vulnerabilidades dos alvos;
2.10.4. Penetração em alvos;
2.10.5. Manipulação no nível do aplicativo;
2.10.6. Engenharia reversa Java / ActiveX do lado do cliente;
2.10.7. Ataques de negação de serviço;
2.10.8. Verificações / explorações perigosas.

3. COMPROVAÇÃO DAS CARACTERÍSTICAS TÉCNICAS

3.1. O não atendimento às especificações técnicas descritas neste EDITAL implicará a desclassificação da proposta apresentada.
3.2. A comprovação do atendimento às características técnicas especificadas neste EDITAL dar-se-á por meio da apresentação de um ou mais casos de sucesso fornecidos por pessoas jurídicas de direito público ou privado e de comprovação de equipe técnica capacitada para execução de atividade pertinente e compatível em características, quantidades e prazos com o objeto da licitação.
3.3. No momento da assinatura do contrato a CONTRATADA deverá apresentar a lista de profissionais, com suas devidas certificações, que irão atuar no Pentest (testes de intrusão/penetração).
3.4. A prestação do Serviço de Teste de intrusão deverá ser realizada por empresa que atenda os seguintes critérios mínimos:
3.4.1. Certificação Ethical Hacking Foundation
3.4.2. Certificação ISO 27001
3.4.3. Equipe de Ethical Hackers com acesso à Deep e Dark para consultar e entender as principais técnicas que vêm sendo utilizadas por hackers ao redor do mundo.
3.4.4. Empresa possuir equipes de Blue Team e Red Team.
3.4.5. Empresa possuir caso de sucesso de suporte à recuperação de ataques cibernéticos.
3.4.6. Empresa possuir pelo menos 3 anos de funcionamento.
3.4.7. Empresa possuir pelo menos 01 atestado técnico de serviços de segurança da informação.

3.5. Os Documentos poderão ser apresentados em original, cópia autenticada ou cópia simples acompanhada do original para conferência pela Comissão.
3.6. As propostas serão analisadas por equipe de técnicos da CONTRATANTE para fins de verificação do atendimento às características da solução especificados neste EDITAL.
3.7. A falta de informações técnicas ou a incompatibilidade destas com as características especificadas implicará a desclassificação da proposta.

4. SIGILO E INVIOLABILIDADE

4.1. A CONTRATADA compromete-se a manter em caráter confidencial as informações abaixo mencionadas, mesmo após a eventual rescisão do contrato:

4.1.1. Política de segurança adotada pelo CONTRATANTE e configurações de hardware e software decorrentes;

4.1.2. Processo de instalação, configuração e customizações de produtos, ferramentas e equipamentos e atendimento aos itens de segurança, constantes do Edital de licitação;

4.1.3. Processo de implantação no ambiente do CONTRATANTE, de mecanismos de criptografia e autenticação utilizados;

4.1.4. Recomendações e implementações decorrentes do processo de consultoria;

4.1.5. Quaisquer dados que a CONTRATADA venha a ter conhecimento em decorrência da presente contratação, pertinentes a hardware, serviços e sistemas aplicativos do CONTRATANTE, cujo conhecimento por terceiros exponha o ambiente a riscos de invasão ou resulte na vulnerabilidade do mesmo.

4.1.6. Não fazer uso das informações prestadas pela CONTRATANTE que não seja em absoluto cumprimento ao contrato em questão.

4.1.7. A quebra da confidencialidade ou sigilo de informações obtidas na prestação de serviços ensejará multa, responsabilidade criminal na forma da lei, sem prejuízo de outras providências nas demais esferas. A CONTRATADA obriga-se a tomar as providências necessárias para assegurar que as informações confidenciais não sejam divulgadas por seus empregados ou agentes.

stefaninirafael

SERVIÇO
Teste de Intrusão e Rastreamento de Vulnerabilidades

CLIENTE
MPBA

MINISTÉRIO PÚBLICO
DO ESTADO DA BAHIA

Proposta Técnica Comercial n° 093708_20210713_2
13 de julho de 2021

Sumário

1. APRESENTAÇÃO 5

2. DADOS DA EMPRESA 6

3. INTRODUÇÃO 7

3.1 ESTRUTURAÇÃO DA PROPOSTA 7

4. SOBRE A STEFANINI RAFAEL 8

4.1 ALGUNS DOS CLIENTES DA STEFANINI RAFAEL 9
4.2 POSICIONAMENTO GLOBAL DA STEFANINI RAFAEL 9
4.3 SERVIÇOS OFERTADOS PELA STEFANINI RAFAEL 10

5. PROPOSTA TÉCNICA 11

5.1 ESCOPO 11
5.1.1 Conteúdo do Edital 11
5.1.2 Restrições ao Teste de Intrusão 12
5.1.3 Produtos de Entrega 13
5.1.4 Estimativa de Prazos 14
5.1.5 Recursos Necessários ao Projeto 14
5.2 METODOLOGIA DE GERÊNCIA DE PROJETO 16

6. RESPONSABILIDADES E PREMISSAS TÉCNICAS 17

6.1 EXCLUSÕES (UNDELIVERABLES) 17
6.2 PREMISSAS GERAIS 17
6.3 PREMISSAS DA CONTRATADA 17
6.4 PREMISSAS DO CONTRATANTE 18
6.5 RESPONSABILIDADES DO CONTRATANTE COM A CONTRATADA 18
6.6 RESPONSABILIDADES DA CONTRATADA COM O CONTRATANTE 18
6.7 DIREITOS DE PROPRIEDADE 19

7. PROPOSTA COMERCIAL 20

8. PREMISSAS COMERCIAIS 21

8.1 CONDIÇÕES DE PAGAMENTO 21
8.2 ÍNDICE DE REAJUSTE 21
8.3 DAS NOTIFICAÇÕES 21
8.4 REEQUILÍBRIO ECONÔMICO 21
8.5 RESCISÃO CONTRATUAL 22

9. TERMO DE ACEITE 23

ANEXO – MODELO DE RELATÓRIO 24

Anexo Orcamento 01.pdf (0164231) SEI 19.09.02684.0011790/2021-22 / pg. 20

Lista de Figuras

Figura 1 - Estrutura de Diretorias 8
Figura 2 - Clientes Stefanini Rafael 9
Figura 3 - Posicionamento global da Stefanini Rafael 9
Figura 4 - Fases PMBok 16
Figura 5 - Etapas de uma Sprint 16

Lista de Tabelas

Tabela 1 – Teste de Intrusão Aplicações Críticas 20

Anexo Orcamento 01.pdf (0164231) SEI 19.09.02684.0011790/2021-22 / pg. 21

Histórico

Data	Autor	Descrição	Versão
22/06/2021	Marco Alexandre Rodrigues	Criação do documento	1.00
13/07/2021	Alex Willian de Oliveira	Revisão da Proposta	2.00

Responsável pela Proposta

E-mail: marco.rodrigues@stefaninirafael.com
Contato: +55 (11) 9 4192-3758

Validade da Proposta

Esta proposta tem validade de **60 dias**, a partir da data da emissão de sua última versão.

Data de emissão: 13/07/2021
Data de validade: 12/09/2021

Anexo Orcamento 01.pdf (0164231) SEI 19.09.02684.0011790/2021-22 / pg. 22

1. APRESENTAÇÃO

Ministério Público da Bahia

Prezados Senhores,

Segue o documento contendo as condições técnicas e comerciais para atendimento da solicitação cliente para o fornecimento de um serviço de teste de intrusão (*Pen Test*) e rastreamento de vulnerabilidades (*Vulnerability Scan*).

Este documento foi elaborado envolvendo as áreas de soluções, negócios e recursos humanos, que trabalhando em equipe criaram esta solução para atender ao requerido.

A Stefanini Rafael possui uma característica de forte adaptação ao cliente e o modelo de negócio apresentado nessa proposta é um primeiro balizador desenhado com premissas que podem ser alteradas caso haja esta necessidade.

Agradecemos o convite para participação nesta oportunidade e esperamos atender a todas as expectativas.

Estaremos à disposição para os esclarecimentos necessários.

Boa leitura.

Atenciosamente,

Leidivino Natal da Silva
CEO – Stefanini Rafael
natal.silva@stefaninirafael.com
+55 11 97130-5514

Anexo Orcamento 01.pdf (0164231) SEI 19.09.02684.0011790/2021-22 / pg. 23

2. DADOS DA EMPRESA

Dados oficiais

Razão Social: Stefanini Rafael Segurança e Defesa S.A.
Nome Fantasia: Stefanini Rafael Segurança e Defesa S.A.
CNPJ: 24.691.488/0001-09
Web Site: www.stefaninirafael.com.br

Matriz

Avenida Eusebio Matoso 1375, 8° Andar Sala 801 e 802
São Paulo UF: SP Cep: 05423-905

CEO

Leidivino Natal da Silva
CEO – Stefanini Rafael
natal.silva@stefaninirafael.com
+55 11 97130-5514

Representante Comercial

Patrícia Maia Dantas
Diretora de Negócios
pmdantas@stefanini.com
+55 71 9 9624-7432

Representantes Legais

Maria Magali Bredariol
Diretora Jurídica
mbredariol@latam.stefanini.com
+55 11 99934-2252

Luiz Carlos Marques de Aguiar
Diretor Financeiro
laguiar@stefanini.com
+55 11 97283-2530

Anexo Orcamento 01.pdf (0164231) SEI 19.09.02684.0011790/2021-22 / pg. 24

3. INTRODUÇÃO

Para atender à solicitação cliente, desenvolvemos uma solução que está apresentada neste documento, que inclui o detalhamento técnico, entrega dos serviços e produtos, incluindo os métodos, ferramentas e equipe ofertada.

Nesta Proposta Técnica, demonstramos como entendemos o desafio apresentado pelo cliente e de como podemos atender a esta demanda, visando atender aos requisitos técnicos conforme solicitado durante reunião com a equipe técnica.

3.1 ESTRUTURAÇÃO DA PROPOSTA

A Proposta Técnica Comercial foi estruturada em documento único e contém o detalhamento do entendimento dos requisitos solicitados, entrega dos serviços e produtos, incluindo os métodos, ferramentas, equipes e infraestrutura ofertadas, além do valor do investimento, termos e condições comerciais.

Anexo Orcamento 01.pdf (0164231) SEI 19.09.02684.0011790/2021-22 / pg. 25

4. SOBRE A STEFANINI RAFAEL

A Stefanini Rafael Segurança e Defesa é uma **joint venture** entre a **Stefanini**, multinacional brasileira que atua no setor de serviços de tecnologia da informação, com a empresa **Rafael Advanced Defense Systems** de origem Israelense e conhecida mundialmente como uma das maiores empresas de soluções em Segurança & Defesa. A Stefanini Rafael Segurança e Defesa tem por objetivo atuar nas áreas de Segurança & Defesa no Brasil e América Latina, com soluções inovadoras e sistemas de alta tecnologia.

A Stefanini Rafael é composta no Brasil da Diretoria se Segurança Cibernética e Inteligência e da Diretoria de Comunicação.

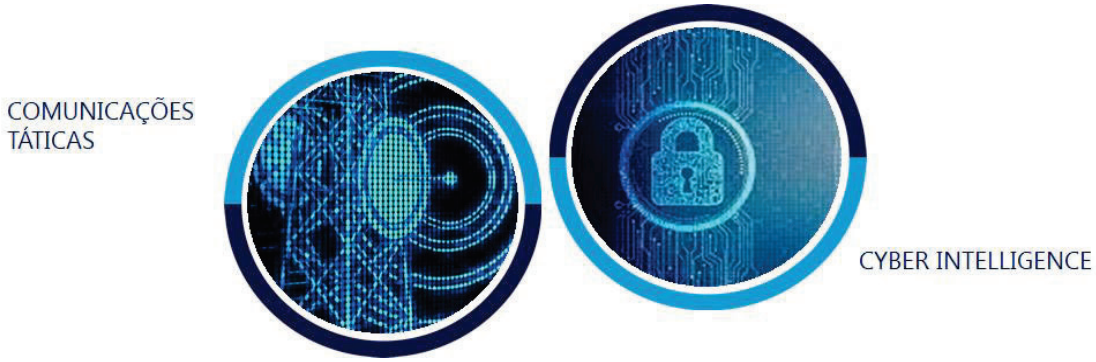


Figura 1 - Estrutura de Diretorias

MISSÃO	ESTRATÉGIA	VISÃO
Trabalhamos para concretizar os sonhos dos nossos clientes, colaboradores e acionistas, através da melhor tecnologia para soluções de Cyber, Segurança, Inteligência e Defesa.	Nossas decisões e nosso comportamento são movidos por valores importantes: agir com integridade, respeito, energia, atitude positiva e foco em resultados sustentáveis.	Com base em nossos valores, buscamos ser o melhor provedor de tecnologia, reconhecido como um parceiro estratégico, por agir com paixão e energia para conquistar e encantar os clientes.

Acesse nosso site e conheça mais em: http://www.stefaninirafael.com

Anexo Orcamento 01.pdf (0164231) SEI 19.09.02684.0011790/2021-22 / pg. 26

4.1 Alguns dos clientes da Stefanini Rafael



Figura 2 - Clientes Stefanini Rafael

4.2 Posicionamento Global da Stefanini Rafael

A Stefanini Rafael tem como foco principal o mercado Brasileiro, porém já estamos posicionados em outros países e com planos de expansão para outros mercados:

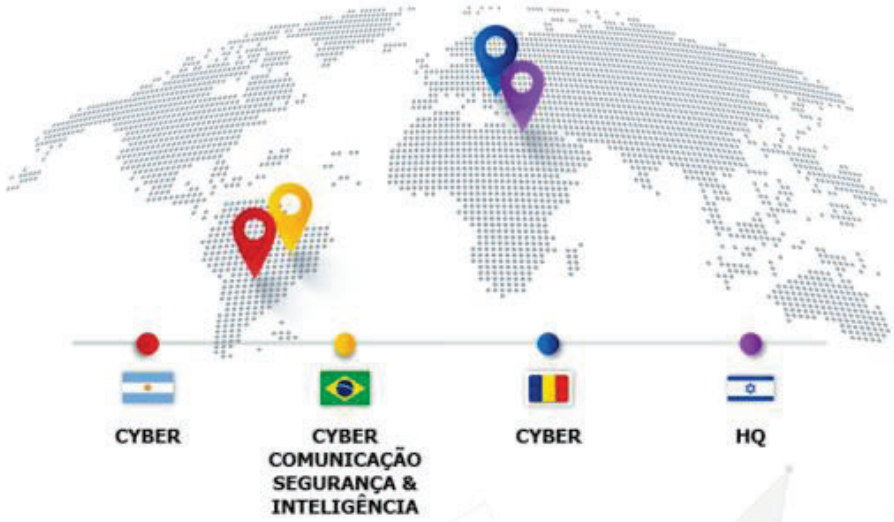


Figura 3 - Posicionamento global da Stefanini Rafael

Anexo Orcamento 01.pdf (0164231) SEI 19.09.02684.0011790/2021-22 / pg. 27

4.3 Serviços ofertados pela Stefanini Rafael

Plano Estratégico	• Desenvolvimento de políticas de segurança da informação; • Gestão de riscos e conformidades; • Auditoria Independente de Segurança da Informação;
Plano Tático	• Consultoria de Segurança da Informação – Governança; • Suporte para certificações como PCI-DSS, ISO 27000/05; • Auditoria Independente de Segurança da Informação; • Venda de produtos e serviços dos maiores players de mercado;
Plano Operacional	• Pentest (Black-Box, White Box e Gray Box); • Teste de vulnerabilidades de softwares e códigos; • Monitoramento de respostas a incidentes de segurança; • Gestão de segurança da informação de empresas clientes; • Alocação de profissionais de segurança no ambiente de T.I. do cliente. (body shop); • Monitoramento e avaliação de riscos de segurança na Deep e na Dark Web; • Treinamentos para clientes.

Anexo Orcamento 01.pdf (0164231) SEI 19.09.02684.0011790/2021-22 / pg. 28

5. PROPOSTA TÉCNICA

Esta proposta técnica visa atender aos requisitos solicitados pelo cliente **Ministério Público da Bahia** para a prestação de serviços técnicos de segurança cibernética. O escopo deve atender ao documento “Especificação Técnica MP BA - Pentest Voto Eletrônico” publicado pelo Contratante.

5.1 Escopo

O escopo técnico desta proposta refere-se à prestação de serviço de teste de intrusão (*Pentest*).

Características deste projeto:

- Teste de Intrusão tipo **Black Box** de **1 aplicações críticas (1x URL)**.
- O serviço será prestado de **forma remota.**
- O cliente deverá preencher **autorização prévia para a realização dos serviços**.

Os produtos finais desta proposta:

- Teste de Intrusão:
  - Identificar modos de explorar as vulnerabilidades a fim de enganar ou anular os recursos de segurança dos componentes do sistema.
  - Cliente deverá identificar os endereços das dez aplicações críticas.

5.1.1 Conteúdo do Edital

Reprodução de conteúdo do documento “Especificação Técnica MP BA - Pentest Voto Eletrônico” publicado pelo Contratante.

A atividade de Teste de Intrusão/Penetração (Pentest) deve compreender o teste de Invasão externa e tem como objetivo principal identificar, possíveis vulnerabilidades na **aplicação WEB** VOTO ELETRÔNICO da CONTRATANTE. Estes testes envolvem o uso de técnicas e ferramentas para tentar o acesso privilegiado aos ativos e informações da CONTRATANTE por meio de simulações controladas de ataques reais, sendo o ambiente da aplicação da CONTRATANTE avaliado em sua totalidade em busca de vulnerabilidades que possam permitir a obtenção de acesso não-autorizado, sendo que a modalidade de teste de intrusão/penetração a ser realizado será do tipo **Black Box**.

O teste Black Box parte da premissa que o profissional não tem informações sobre o sistema nem da estrutura da empresa e trata a aplicação como uma “caixa preta”. Sendo mais difícil de ser aplicado, já que é preciso colher algumas informações para tentar explorar vulnerabilidades, mas em compensação, essa simulação fica mais próxima de um ataque real feito externamente por um hacker.

A CONTRATADA deverá realizar **1 teste intrusão** para identificação de vulnerabilidades por meio de simulações de invasão de serviços e infraestrutura (Teste de Invasão) a serem executadas externamente (através da Internet), com duração de **até 20 (vinte) dias**.

A CONTRATADA deverá elaborar “Relatório de Teste de Invasão” para cada teste realizado apresentando todas as informações sobre o mesmo, contemplando no mínimo: objetivos, premissas e escopo do teste; metodologia de análise de

vulnerabilidades; descrição das ações realizadas; vulnerabilidades encontradas; categorização e severidade das vulnerabilidades, recomendações e controles de segurança necessários para correção das vulnerabilidades; apresentação das evidências; referências e ferramentas utilizadas.

A Metodologia adotada pela CONTRATADA durante o Pentest deve incluir minimamente, quando pertinente, as seguintes vulnerabilidades:

1. Injeção de Código.
2. Quebra de Autenticação.
3. Exposição de Dados Sensíveis.
4. Entidades Externas de XML.
5. Quebra de Controle de Acesso.
6. Configuração Incorreta de Segurança.
7. Cross-Site Scripting (XSS).
8. Desserialização Insegura.
9. Utilização de Componentes com Vulnerabilidades Conhecidas.
10. Log e Monitoramento Ineficientes.

A CONTRATADA deverá minimamente compreender atividades que busquem encontrar vulnerabilidades em potencial, de eventual má configuração, de falhas em hardwares e softwares desconhecidos, de técnicas de contramedidas ou deficiências na infraestrutura ou sistemas da CONTRATANTE.

A CONTRATANTE deve criar **um usuário interno para a CONTRATADA** no ambiente da CONTRATANTE com todas suas ações logadas para documentação e atestar a integridade do trabalho realizado pela CONTRATADA.

O alvo do PENTEST (Teste de Invasão) será a aplicação aqui denominada VOTO ELETRÔNICO. Todas as fases dos PENTEST poderão ser acompanhadas e supervisionadas a qualquer momento pelo CONTRATANTE. Quaisquer atividades com suspeita de comprometimento de algum ambiente ou ativo, deverá a CONTRATADA ser reportada pelo CONTRATANTE.

Os serviços contratados deverão ser obrigatoriamente executados fora das dependências da CONTRATANTE.

O teste de penetração incluirá as seguintes técnicas de teste:

- Ping sweep de intervalos de redes;
- Verificação de portas de hosts de destino;
- Verificação de vulnerabilidades dos alvos;
- Penetração em alvos;
- Manipulação no nível do aplicativo;
- Engenharia reversa Java / ActiveX do lado do cliente;
- Ataques de negação de serviço;
- Verificações / explorações perigosas.

5.1.2 Restrições ao Teste de Intrusão

Os métodos, técnicas e ferramentas deverão ser selecionadas pelo *Ethical Hacker*, conforme o escopo, o tipo de aplicação e as restrições impostas pelo cliente. Não há a

obrigatoriedade de utilizar todos os métodos, técnicas e ferramentas para todos os projetos.

Os métodos, técnicas e ferramentas apresentados, podem afetar a performance e até mesmo interromper o uso de alguns equipamentos momentaneamente. Desta forma, a escolha dos métodos e técnicas deverão ser avaliados conforme cada cliente, infraestrutura, severidade dos testes e importância dos equipamentos.

Métodos que aplicam dicionário de senhas e *brute force* tendem a ser mais agressivos ao ponto de afetar os equipamentos servidores. Não há nestes casos, como garantir que o teste não afetara o servidor/sistema.

No entanto vale ressaltar que estes testes apresentam respostas muito positivas no contexto da análise de intrusão e são métodos comuns e muito usados por Black Hackers. Assim o teste de intrusão com estes testes serve também para mostrar a resiliência do servidor/sistema ante a ataques similares no mundo real.

Uma opção para mitigar este problema é agendar os testes nos horários com menor uso e tráfego de dados pelos servidores, evitando a queda de performance ou indisponibilidade.

Outro ponto importante é que toda ação da equipe Stefanini Rafael, só será realizada após autorização formal do cliente, com o consentimento de execução, os riscos conhecidos, o tipo de teste e os horários programados de execução.

5.1.3 Produtos de Entrega

Os produtos de entrega previstos (*Deliverables*), consistem em um relatório que deverá reportar as estratégias e métodos utilizados para realizar a análise de segurança e os resultados de vulnerabilidades encontradas, assim como sugestões pra a equipe técnica do cliente.

O relatório do Teste de Intrusão deve conter a descrição de cada problema verificado e/ou possível problema descoberto. Riscos mais específicos que a vulnerabilidade pode representar, incluindo métodos específicos como e até que ponto ele pode ser explorado (Eliminação, mitigação, aceitação). Exemplos de vulnerabilidades incluem, entre outros, injeção de SQL, escalonamento de privilégio, script entre sites ou protocolos obsoletos.

O relatório do Rastreamento de Vulnerabilidades deve evidenciar os riscos potenciais apresentados por vulnerabilidades conhecidas, classificados de acordo com as pontuações associadas a cada vulnerabilidade.

Os relatórios finais têm por objetivo:

- Relatar os resultados obtidos.
- Dar suporte à equipe de segurança e de operação para solucionar os principais problemas de segurança no ambiente.
- Servir como métrica para medir à maturidade do negócio da empresa e a sua importância com a segurança, além de medir o trabalho da equipe de segurança sobre a aplicação das melhores práticas de proteção.
- Servir como uma prova dos testes realizados e de que tudo foi devidamente realizado sem fugir do escopo determinado.

Anexo Orcamento 01.pdf (0164231) SEI 19.09.02684.0011790/2021-22 / pg. 31

- Prover informações relevantes sobre os testes realizados no ambiente caso haja um incidente durante ou posteriormente, após os testes de vulnerabilidade.

5.1.4 Estimativa de Prazos

As entregas referentes a esta proposta devem seguir aos prazos aqui estimados para a análise em um web site (URL), uma API ou um Aplicativo Móvel:

Método Black Box
- 40 a 80 horas de execução
- Realização estimada em 10 - 20 dias úteis consecutivos

5.1.5 Recursos Necessários ao Projeto

Detalha-se a seguir a infraestrutura necessária para este projeto.

5.1.5.1 Acessos
Para melhor entregar e testar as vulnerabilidades existentes no ambiente do cliente será necessário um usuário com poder administrativo na árvore de domínio. Dessa maneira será possível acessar vulnerabilidades que são encontradas dentro de sistemas operacionais dos dispositivos existentes no ambiente de rede. Esta exigência está atrelada a análise de rede interna e depende do método de análise escolhido.

5.1.5.2 Infraestrutura
O cliente deve prover à Stefanini Rafael, caso necessário, um ambiente de trabalho para a equipe técnica que necessitar trabalhar alocada na estrutura física do cliente, como mesas, cadeiras, entradas de energia e conexões à rede tantas quanto forem necessárias.

Este ambiente deve ser restrito e em local afastado dos demais colaboradores para evitar que as informações coletadas durante o processo de análise de vulnerabilidades percam a confidencialidade, pois podem trazer informações sensíveis ao ambiente e causar dados irreparáveis tanto ao ambiente quanto à integridade do cliente.

5.1.5.3 Autorizações
O cliente deve prover à Stefanini Rafael, caso necessário, autorização formal para acesso ao ambiente digital onde serão realizadas as análises.

5.1.5.4 Questionário Inicial
O cliente deve prover à Stefanini Rafael, o documento intitulado “Questionário de Pen Test”, para que nossos especialistas possam preparar melhor a estratégia de análise a ser aplicada.

Exemplos de algumas questões relativas ao processo de análise:
- Quais hosts específicos, intervalos de endereços de rede ou aplicativos devem ser testados?
- Quais hosts específicos, intervalos de endereços de rede ou aplicativos não devem ser explicitamente testados?
- O teste será realizado em um ambiente de produção ao vivo ou em um ambiente de teste?
- Os ataques de negação de serviço são permitidos?

- As verificações e explorações perigosas são permitidas?

Anexo Orcamento 01.pdf (0164231) SEI 19.09.02684.0011790/2021-22 / pg. 33

5.2 Metodologia de Gerência de Projeto

Todos os projetos da Stefanini Rafael utilizam os preceitos do Guia PMBOK (*Project Management Body of Knowledge*), que consiste em uma publicação do *Project Management Institute*, PMI, que compila as melhores práticas mundialmente aceitas em Gerenciamento de Projetos.

O Guia PMBOK identifica um subconjunto de conhecimentos em gerenciamento de projetos, que é amplamente reconhecido como boas práticas. Uma boa prática não significa que o conhecimento e as práticas devem ser aplicados uniformemente a todos os projetos, sem considerar se são ou não apropriados.

O Guia PMBOK também fornece e promove um vocabulário comum para se discutir, escrever e aplicar o gerenciamento de projetos possibilitando o intercâmbio eficiente de informações entre os profissionais de gerência de projetos.

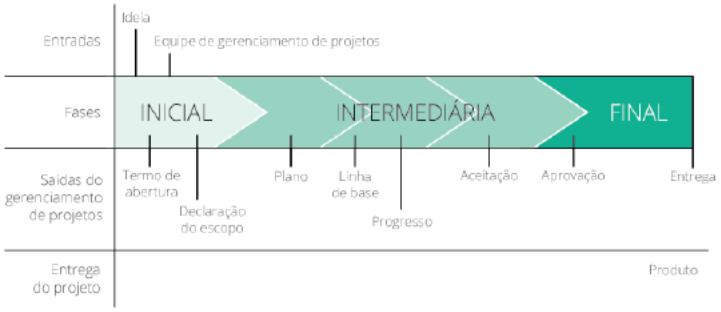


Figura 4 - Fases PMBok

Para projetos que envolvem o desenvolvimento de sistemas ou alocação de *squads* no cliente, a gestão de projetos pode ainda associar o *Framework Scrum* para a gestão com o Conceito Ágil.



Figura 5 - Etapas de uma Sprint

Anexo Orcamento 01.pdf (0164231) SEI 19.09.02684.0011790/2021-22 / pg. 34

6. RESPONSABILIDADES E PREMISSAS TÉCNICAS

Para este capítulo devemos considerar a nomenclatura:

- Contratante: Cliente ou empresa contratante do serviço.
- Contratada: Prestador do serviço contratado.
- Partes: Ambas as empresas. Responsabilidade de ambas as partes.

6.1 Exclusões (Undeliverables)

- Este serviço não prevê análises Antispam ou de Phishing em repositórios ou domínios de e-mail.
- Este serviço não prevê a execução de atividades de correção ou de mitigação de riscos, sendo o objeto desta proposta apenas a avaliação das informações, testes, análise documental e entrega dos relatórios finais para o cliente com as proposições de melhorias.

6.2 Premissas Gerais

- Todas as atividades apresentadas nesta proposta consideram a efetiva participação do Contratante.
- É de responsabilidade das Partes a não divulgação de dados ou informações relacionadas aos produtos objetos do presente, mantendo sigilo absoluto em relação a todos os dados acessados ou que venham a ser gerados no processo de prestação dos serviços. Desta forma, todos os documentos relativos a este projeto, incluindo esta proposta, estão classificados como documento confidencial.
- As datas, horários e cronograma para a execução das atividades aqui propostas serão devidamente acordados entre as Partes, após a assinatura do contrato.
- As estimativas de tempo e custo desta proposta foram criadas com base nas informações fornecidas pelo Contratante durante a elaboração deste documento, de forma que o escopo a ser executado é o descrito neste documento.
- Caso haja a necessidade de executar atividades fora dos horários comerciais ou em finais de semana ou feriados, deverá ocorrer acréscimos nos valores da mão de obra, conforme previsto na legislação trabalhista atual.
- Caso haja necessidade de incorrer em custos adicionais, a Contratada só o fará com a anuência do Contratante.

6.3 Premissas da Contratada

- A execução das atividades previstas nesta proposta já confere automaticamente a autorização para o pagamento.
- O gerente de projetos e/ou gerente de delivery da Contratada terá independência para gerenciar toda a sua equipe.
- As horas improdutivas são caracterizadas pelas situações onde os consultores da Contratada estão disponíveis para realizar as suas atividades, mas os trabalhos não podem evoluir por conta de um eventual descumprimento de cronograma por parte do Contratante, como: falta no fornecimento de informações, pré-requisitos e premissas não atendidos, indisponibilidade de

Anexo Orcamento 01.pdf (0164231) SEI 19.09.02684.0011790/2021-22 / pg. 35

equipamentos, indisponibilidade de pessoal do cliente, indisponibilidade de outros fornecedores do cliente que estejam envolvidos nas atividades de projeto, dentre outros aspectos similares. Horas improdutivas contam como tempo de projeto para o cálculo dos honorários em favor da Contratada.

- Integrantes do time Contratante não poderão ser contratados ou terceirizados pela Contratante, seja dentro do período de prestação dos serviços, ou em até 3 (três) meses após a entrega dos serviços contratados, sob pena de indenização correspondente à média dos últimos 3 (três) meses de serviços prestados.

6.4 Premissas do Contratante

- Integrantes do time Contratada não poderão ser contratados ou terceirizados pela Contratante, seja dentro do período de prestação dos serviços, ou em até 3 (três) meses após a entrega dos serviços contratados, sob pena de indenização correspondente à média dos últimos 3 (três) meses de serviços prestados.

6.5 Responsabilidades do Contratante com a Contratada

- Designar um colaborador principal (Preposto) que será o ponto focal com o time da Contratada. Este preposto deverá ter poder de decisão e acessos executivos que vierem a ser necessários. Responsabilidades:
  - Acompanhamento dos serviços,
  - Agendamento de interações com equipes internas,
  - Resolução de situações que possam gerar atrasos ou problemas ao projeto,
  - Designar novo preposto em situações de férias ou ausências temporárias.
- Fornecer todas as informações necessárias e pertinentes ao assunto, em tempo hábil, sem qualquer forma de reserva ou censura.
- Disponibilizar a infraestrutura necessária (sala de reunião, mesas, cadeiras) para o desenvolvimento dos trabalhos, de acordo com a necessidade.
- Disponibilizar pessoas responsáveis pelos processos, as quais possam apoiar nossos engenheiros a entender a topologia de rede ou aplicações do cliente.
- Disponibilidade de equipe local de apoio durante as visitas de nossa equipe no local.
- Fornecer às nossas equipes usuários e permissões de acesso conforme necessário.
- Fornecer às nossas equipes arquitetura e topologia de rede do sistema, lista de fornecedores de soluções de terceiros e mecanismos de integração conforme necessário.
- Fornecer todas as informações necessárias e pertinentes ao assunto, em tempo hábil, sem qualquer forma de reserva ou censura.
- Disponibilizar a infraestrutura necessária (sala de reunião, mesas, cadeiras) para o desenvolvimento dos trabalhos, de acordo com a necessidade.

6.6 Responsabilidades da Contratada com o Contratante

- Contratar profissionais qualificados, compatíveis com a complexidade e atribuições dos serviços apresentados nessa proposta.
- Assegurar a boa conduta dos profissionais, considerando sempre as políticas internas do cliente.

6.7 Direitos de propriedade

Todos os relatórios ou documentos gerados durante esse serviço serão de propriedade exclusiva do Contratante.

Anexo Orcamento 01.pdf (0164231) SEI 19.09.02684.0011790/2021-22 / pg. 37

7. 0.312PROPOSTA COMERCIAL

Os valores apresentados nas tabelas abaixo referem-se aos métodos aplicáveis de Testes de Intrusão, cada qual com suas características técnicas e particularidades.

Prestação de Serviços Técnicos Teste de Intrusão (Pentest) Aplicação Web	**Preço Total**
Método Black Box (40 horas de execução)	R$ 8.202,67
Análise de um endereço Web (URL)	
Incluso análise em até três APIs por endereço Web	

Tabela 1 – Teste de Intrusão Aplicações Críticas

Para aplicações críticas (Web), os valores apresentados na tabela 1, se referem a uma única Aplicação Web (URL), com a análise de no máximo três APIs.

As opções apresentadas na Tabela 1 representam a aplicação do Teste de Intrusão uma única vez, para uma aplicação crítica.

Caso haja necessidade de testes mais complexos, com um número maior de APIs, existe a possibilidade de um ajuste nos valores apresentados nesta tabela, o qual será objeto de nova proposta.

Faz-se mister ressaltar que estas análises podem também concluir que o cliente não possui vulnerabilidades na aplicação analisada. Este é um risco que pode ocorrer neste processo, e que neste caso, mostraria que a aplicação do cliente está atualizada e aderente aos melhores padrões de segurança do mercado.

Anexo Orcamento 01.pdf (0164231) SEI 19.09.02684.0011790/2021-22 / pg. 38

8. PREMISSAS COMERCIAIS

8.1 Condições de Pagamento

Seguem condições:

- As notas fiscais deverão ser emitidas no 1º dia útil de cada mês subsequente à prestação do serviço.
- Prazo de vencimento será de até 15 dias da data de sua emissão.
- Todos os impostos estão inclusos no preço apresentado (ISS, IR, PIS, COFINS, CSSL).
- O pagamento será realizado através depósito bancário (transferência, DOC ou TED).
- Qualquer quantia que não seja paga na data do vencimento combinado será acrescida de correção monetária, calculada de acordo com a variação do IPCA-IBGE, e juros de mora de 1% (um por cento) ao mês, tudo corrigido, *pro-rata temporis*, além do pagamento de multa moratória no importe de 2% (dois por cento) dos valores em atraso, que serão imediatamente devidos e pagáveis à Stefanini Rafael.

8.2 Índice de Reajuste

Os preços dos serviços serão reajustados anualmente, a partir da assinatura do contrato/aditivo, na variação positiva do IGPM anual e/ou índice de mercado.

8.3 Das Notificações

Eventuais retenções, deduções ou compensações previstas no presente instrumento contratual, somente serão válidas e se concretizarão quando da prévia notificação por escrito, com antecedência mínima de 15 (quinze) dias corridos à Contratada, explicitando detalhadamente os motivos pelos quais tais ações serão praticadas.

As retenções, deduções ou compensações somente ocorrerão após a possibilidade de defesa da Contratada, garantindo-se o direito à ampla defesa e ao contraditório dentro de prazo razoável. Qualquer retenção arbitrária por parte da Contratante ensejará na devolução imediata do valor retido à Contratada, bem com multa de 15% sobre o valor retido, sem prejuízos das perdas e danos.

8.4 Reequilíbrio Econômico

Em caso de alterações de ordem econômica advindas de medidas governamentais futuras ou quanto a legislação tributária e/ou previdenciária em vigor nesta data, de modo a modificar, majorar ou reduzir os tributos e encargos incidentes sobre as operações aqui pactuadas, assim como pela instituição ou extinção de outros impostos, taxas, contribuições especiais de qualquer natureza, restituíveis ou não, que venham a incidir ou repercutir sobre este ajuste e/ou seu objeto, a Stefanini Rafael atualizará os valores contratuais e informará à Contratante, de forma a manter o equilíbrio econômico-financeiro do contrato, conforme disposto nos artigos 478 e 479 do código civil brasileiro.

8.5 Rescisão Contratual

Poderá o contrato ser cancelado por instrumento consensual firmado entre as Partes, nas condições pactuadas pelas mesmas na ocasião do cancelamento.

As Partes poderão rescindir o presente contrato, independentemente de qualquer notificação judicial ou extrajudicial, nas seguintes hipóteses:

I. Inadimplência reiterada de qualquer cláusula ou condição do presente contrato, não sanada no prazo estabelecido em notificações prévias.
II. Decretação de falência, insolvência ou recuperação judicial da Contratada ou da Contratante.
III. Nos demais casos previstos na legislação em vigor.
IV. Atraso nos pagamentos combinados, superiores a 30 (trinta) dias, contados dos respectivos vencimentos, pela Contratante.

9. TERMO DE ACEITE

Data da Proposta
julho 14, 2021

Nome

Cargo

Assinatura Data / /

☐ Aceito os termos

Aplicação Críticas - Descrever a URLs / IPs:

Aplicação de voto eletrônico

URL:

Range de IPs:

Tipo de Teste:

☐ White Box ☐ Grey Box ☒ Black Box

Anexo Orcamento 01.pdf (0164231) SEI 19.09.02684.0011790/2021-22 / pg. 41

ANEXO – MODELO DE RELATÓRIO



Relatório de Pentest – Target a ser testado

Versão: 1.00 Sigiloso - Restrito

stefaninirafael

Documento	Emitido em	Responsável
Relatório de Pentest – Target a ser testado	DD-Mês-AAAA	Nome do responsável pelo teste
Cliente	**Projeto**	
Empresa X	Pentest – target a ser testado	

Sumário

1. OBJETIVO 4

2. INTRODUÇÃO 5

3. ESCOPO DO PENTEST 6

3.1 EXCLUSÕES DO ESCOPO DE PENTEST 7

4. VULNERABILIDADES DOS ATIVOS 8

5. VULNERABILIDADES EXPLORADAS 9

5.1 VULNERABILIDADES WEB E DE INFRAESTRUTURA 9

5.1.1 Vulnerabilidades de Risco Alto 9

5.1.1.1 Dispositivos com SSLv3 e/ou TLSv1.0 habilitados 9

5.1.2 Vulnerabilidades de Nível Médio 9

5.1.2.1 Equipamentos com CVEs relacionados a patches de atualização pendentes: 9

5.1.2.2 Arquivos Javascript e JSON expostos na aplicação: 10

5.1.2.3 Enumeração da versão do OpenSSH disponível 10

5.1.3 Vulnerabilidades de Nível Baixo 11

5.1.3.1 URLs com falta de header de prevenção à X-Frame: 11

5.1.3.2 Cookie não tem flag HttpOnly 11

5.1.3.3 Cookie não tem flag Secure 11

5.1.3.4 Cookie de sessão sem expiração 12

5.2 VULNERABILIDADES DO APLICATIVO 12

5.2.1 Vulnerabilidades de Risco Alto 12

5.2.1.1 Aplicativo com mais permissionamentos que o necessário: 12

5.2.1.2 Aplicativo sem restrições de configurações: 12

ANEXO A – PENTEST DD DE MÊS DE AAAA 13

QUESTIONÁRIO DE ESCOPO DE PENTEST: 13

EVIDÊNCIAS DAS VULNERABILIDADES EXPLORADAS: 13

Anexo Orcamento 01.pdf (0164231) SEI 19.09.02684.0011790/2021-22 / pg. 43

stefaninirafael

Documento	Emitido em	Responsável
Relatório de Pentest – Target a ser testado	DD-Mês-AAAA	Nome do responsável pelo teste
Cliente	**Projeto**	
Empresa X	Pentest – target a ser testado	

Histórico

Data	Autor	Aprovador	Descrição	Versão
Dd/mm/aaaa	Nome do autor	N/A	Criação do documento	1.00

Anexo Orcamento 01.pdf (0164231) SEI 19.09.02684.0011790/2021-22 / pg. 44

stefaninirafael

Documento	Emitido em	Responsável
Relatório de Pentest – Target a ser testado	DD-Mês-AAAA	Nome do responsável pelo teste
Cliente	**Projeto**	
Empresa X	Pentest – target a ser testado	

1. OBJETIVO

O objetivo deste documento é apresentar o resultado técnico da avaliação da execução de Pentest e Scan de Vulnerabilidades executado nas URLs e APIs que compõe o aplicativo da Empresa X.

Este documento apresentará o escopo da execução de Pentest e Scan de Vulnerabilidades de acordo com o Questionário de Escopo de Pentest respondido pelo responsável técnico da Empresa X, além disso, será apresentado o resultado da análise e evidências de vulnerabilidades encontradas na infraestrutura, website e Aplicativo da Empresa X.

Anexo Orcamento 01.pdf (0164231) SEI 19.09.02684.0011790/2021-22 / pg. 45

stefaninirafael

Documento	Emitido em	Responsável
Relatório de Pentest – Target a ser testado	DD-Mês-AAAA	Nome do responsável pelo teste
Cliente	**Projeto**	
Empresa X	Pentest – target a ser testado	

2. INTRODUÇÃO

A Empresa X, com o intuito identificar e mapear vulnerabilidades em seu website/rede/aplicativo móvel, firmou através de um contrato uma parceria com à Stefanini Rafael, que tem como objetivo analisar, identificar e mapear vulnerabilidades no aplicativo da Empresa X, utilizando de técnicas de testes de invasão (Pentest). Para esta parceria, contemplado no escopo deste projeto, a Empresa X visa compreender se seu aplicativo apresenta fragilidades e possibilidades de estarem expostos a ataques cibernéticos.

Este relatório irá apresentar o resultado de análise de pentest e de scan de vulnerabilidades.

Anexo Orcamento 01.pdf (0164231) SEI 19.09.02684.0011790/2021-22 / pg. 46

stefaninirafael

Documento	Emitido em	Responsável
Relatório de Pentest – Target a ser testado	DD-Mês-AAAA	Nome do responsável pelo teste
Cliente	**Projeto**	
Empresa X	Pentest – target a ser testado	

3. ESCOPO DO PENTEST

Para definição do tipo de Pentest e o escopo de atuação utilizamos as respostas do Questionário de escopo de Pentest, disponível na seção de Anexo I deste documento. Após análise do questionário respondido, solicitamos recursos para acesso ao ambiente e iniciamos o trabalho.

O trabalho inicial do Pentest é identificar a quantidade de ativos, mapear os ativos críticos ou que não necessitam de avaliação.

Após o mapeamento dos ativos da rede informada ou da unidade de negócio, definimos que o escopo de trabalho do Pentest será avaliar os ativos mapeados.

Desta forma, na Tabelas abaixo, apresentamos todos os ativos mapeados que serão escopo do Pentest.

Aplicativos
Aplicativo 1.apk/.ipa

Tabela 1 - Aplicativos

URL	IP
Urlteste.com.br	100.0.0.1

Tabela 2 - Mapeamento de URLs

Ativos de rede	IP
Ativo 1	10.0.0.1
Ativo 2	10.0.0.2
Ativo 3	10.0.0.3

Tabela 3 - Mapeamento de ativos de rede

Anexo Orcamento 01.pdf (0164231) SEI 19.09.02684.0011790/2021-22 / pg. 47

stefaninirafael

Documento	Emitido em	Responsável
Relatório de Pentest – Target a ser testado	DD-Mês-AAAA	Nome do responsável pelo teste
Cliente	**Projeto**	
Empresa X	Pentest – target a ser testado	

3.1 Exclusões do escopo de pentest

Ativos de rede	IP
Ativo 1	10.0.0.1
Ativo 2	10.0.0.2
Ativo 3	10.0.0.3

Tabela 4 - Ativos Excluídos do teste

Anexo Orcamento 01.pdf (0164231) SEI 19.09.02684.0011790/2021-22 / pg. 48

stefaninirafael

Documento	Emitido em	Responsável
Relatório de Pentest – Target a ser testado	DD-Mês-AAAA	Nome do responsável pelo teste
Cliente	**Projeto**	
Empresa X	Pentest – target a ser testado	

4. VULNERABILIDADES DOS ATIVOS

Após mapeados todos os recursos do aplicativo da Empresa X, iniciamos o trabalho para identificar vulnerabilidades neles.

Executamos ferramentas e scripts e verificamos que existem vulnerabilidades no aplicativo da Empresa X às quais precisam ser tratadas a fim de prevenir possíveis invasões e/ou roubos de informações. As vulnerabilidades encontradas serão descritas nas sessões subsequentes deste relatório com base em sua criticidade em relação ao vazamento de informações.

Quantidade Total	Quantidade	Nível de Risco	Vulnerabilidade
12	1	Médio	Dispositivos com falta de aplicação de patches de atualização e segurança
	11	Médio	Arquivos Javascript e JSON expostos no website
2	1	Baixo	Servidor web sem Flags de segurança setadas
	1	Baixo	Cookie de sessão sem tempo de expiração

Tabela 5 - Vulnerabilidades web e de Infraestrutura

Quantidade Total	Quantidade	Nível de Risco	Vulnerabilidade
6	4	Alto	Aplicativo com mais permissionamentos que o necessário
	2	Alto	Aplicativo sem restrições de configurações

Tabela 6 - Vulnerabilidades do aplicativo

Anexo Orcamento 01.pdf (0164231) SEI 19.09.02684.0011790/2021-22 / pg. 49

stefaninirafael

Documento	Emitido em	Responsável
Relatório de Pentest – Target a ser testado	DD-Mês-AAAA	Nome do responsável pelo teste
Cliente	**Projeto**	
Empresa X	Pentest – target a ser testado	

5. VULNERABILIDADES EXPLORADAS

5.1 Vulnerabilidades web e de Infraestrutura

5.1.1 Vulnerabilidades de Risco Alto

5.1.1.1 Dispositivos com SSLv3 e/ou TLSv1.0 habilitados

Foram encontrados diversos equipamentos com SSLv3 e/ou TLSv1.0 habilitados.
Por se tratar de protocolos já extintos, esta vulnerabilidade permite a quebra de criptografia do tráfego de informações nos dispositivos em questão, consequentemente, as informações uma vez em texto limpo, podem ser capturadas e vazadas na rede mundial de computadores (internet).
As evidências relacionadas a esta vulnerabilidade estão presentes no Anexo I na última sessão deste relatório.

Solução: Habilitar as versões do TLSv1.1 ou superior nos dispositivos e desabilitar o SSLv3 e TLSv1.0 dos mesmos.
.

5.1.2 Vulnerabilidades de Nível Médio

5.1.2.1 Equipamentos com CVEs relacionados a patches de atualização pendentes:

Foram identificados CVEs provenientes da falta de aplicação de atualizações nos equipamentos que hospedam a aplicação. A falta destes patches pode expor informações internas no equipamento em questão
As evidências relacionadas a esta vulnerabilidade estão presentes no Anexo I na última sessão deste relatório.

Solução: Aplicar os paches de atualização e segurança pendentes nos equipamrentos.

Anexo Orcamento 01.pdf (0164231) SEI 19.09.02684.0011790/2021-22 / pg. 50

stefaninirafael

Documento	Emitido em	Responsável
Relatório de Pentest – Target a ser testado	DD-Mês-AAAA	Nome do responsável pelo teste
Cliente	**Projeto**	
Empresa X	Pentest – target a ser testado	

5.1.2.2 Arquivos Javascript e JSON expostos na aplicação:

Foram identificados arquivos Javascript e JSON expontos na aplicação que poder ser manipulados e utilizados para obter informações do sistema e/ou aplicativo.
As evidências relacionadas a esta vulnerabilidade estão presentes no Anexo I na última sessão deste relatório.

Solução: Adicionar os caminhos/extensões no arquivo robots.txt para que estes arquivos não fiquem mais visíveis.

5.1.2.3 Enumeração da versão do OpenSSH disponível

Foi possível enumerar a versão do SSH em alguns equipamentos. Com esta informação é possível explorar ataques de autenticação anônima e brute forcing nos mesmos, a fim de conseguir acesso ao equipamento e, posteriormente, realizar a coleta de informações sensíveis do ambiente.
As evidências relacionadas a esta vulnerabilidade estão presentes no Anexo I na última sessão deste relatório.

Solução: Desabilitar o banner com a versão do SSH e filtrar a conexão apenas para hosts internos.

Anexo Orcamento 01.pdf (0164231) SEI 19.09.02684.0011790/2021-22 / pg. 51

stefaninirafael

Documento	Emitido em	Responsável
Relatório de Pentest – Target a ser testado	DD-Mês-AAAA	Nome do responsável pelo teste
Cliente	**Projeto**	
Empresa X	Pentest – target a ser testado	

5.1.3 Vulnerabilidades de Nível Baixo

5.1.3.1 URLs com falta de header de prevenção à X-Frame:

O header de prevenção à X-Frame não está presente no website, o que permite a um atacante a incorporação da página em uma página falsa, onde o mesmo pode obter dados e informações sigilosas e pessoais da empresa.
As evidências relacionadas a esta vulnerabilidade estão presentes no Anexo I na última sessão deste relatório.

Solução: Adicionar o header de prevenção à ataques do tipo X-Frame.

5.1.3.2 Cookie não tem flag HttpOnly

Quando um cookie possuir a flag HttpOnly, instrui o navegador que o cookie só pode ser acessado pelo servidor e não por client-side scripts. Esta é uma proteção de segurança importante para cookies de sessão.
As evidências relacionadas a esta vulnerabilidade estão presentes no Anexo I na última sessão deste relatório.

Solução: Adicionar flag HttpOnly para os cookies
https://owasp.org/www-community/HttpOnly

5.1.3.3 Cookie não tem flag Secure

Quando um cookie possuir flag Secure, ela instrui o navegador que o cookie só poderá ser acessado com canais seguros SSL/TLS. Esta é uma proteção de segurança importante para cookies de sessão.
As evidências relacionadas a esta vulnerabilidade estão presentes no Anexo I na última sessão deste relatório.

Solução: Adicionar flag Secure para os cookies
https://owasp.org/www-community/controls/SecureFlag

Anexo Orcamento 01.pdf (0164231) SEI 19.09.02684.0011790/2021-22 / pg. 52

5.1.3.4 Cookie de sessão sem expiração

Quando um cookie de sessão não possui tempo de expiração definido, há possibilidade de iniciar ataques de força bruta e de alterações de requisições para o website se utilizando deste recurso.
As evidências relacionadas a esta vulnerabilidade estão presentes no Anexo I na última sessão deste relatório.

Solução: Adicionar tempo de expiração para o cookie de sessão do website.

5.2 Vulnerabilidades do Aplicativo

5.2.1 Vulnerabilidades de Risco Alto

5.2.1.1 Aplicativo com mais permissionamentos que o necessário:

Foi identificado que o aplicativo mobile possui mais permissionamentos que o necessário para seu devido funcionamento. O que permite que o mesmo acesso diversas funções
As evidências relacionadas a esta vulnerabilidade estão presentes no Anexo I na última sessão deste relatório.

Solução: Restringir os acessos do aplicativo para que o mesmo solicite a permissão do usuário para acesso aos dados do aparelho.

5.2.1.2 Aplicativo sem restrições de configurações:

Foi identificado que o aplicativo mobile está com todas as configurações de conexões habilitadas por default o que possibilita o rastreio do aparelho e envio de dados sem quaisquer bloqueios. O que pode ser utilizado por um atacante para envio de requisições falsas e obtenção de informações internas do aplicativo.

Solução: Restringir as configurações do aplicativo para que o mesmo realize as devidas conexões e envio de dados de maneira segura e apenas quando necessário.

Anexo Orcamento 01.pdf (0164231) SEI 19.09.02684.0011790/2021-22 / pg. 53

stefaninirafael

Documento	Emitido em	Responsável
Relatório de Pentest – Target a ser testado	DD-Mês-AAAA	Nome do responsável pelo teste
Cliente	**Projeto**	
Empresa X	Pentest – target a ser testado	

ANEXO A – PENTEST DD DE MÊS DE AAAA

Questionário de escopo de pentest:

Segue abaixo o questionário de escopo de Pentest preenchido pela Empresa X:

Inserir documento preenchido pela Empresa X.

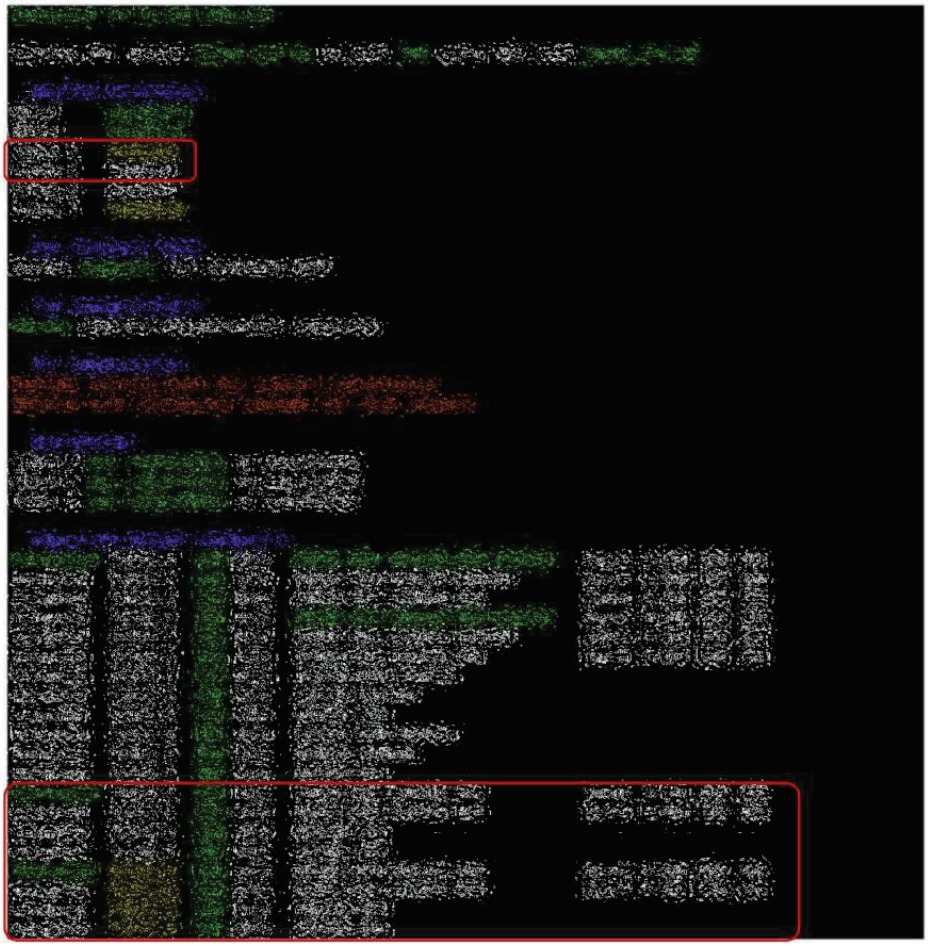
Evidências das vulnerabilidades exploradas:

A seguir seguem as evidências das vulnerabilidades encontradas no ambiente e presentes neste relatório de PenTest. O mesmo foi realizado no período de DD de Mês de AAAA à DD de Mês de AAAA e entregue ao responsável pelo projeto na data de DD de Mês de AAAA.

Anexo Orcamento 01.pdf (0164231) SEI 19.09.02684.0011790/2021-22 / pg. 54

stefaninirafael

Documento	*Emitido em*	*Responsável*
Relatório de Pentest – Target a ser testado	DD-Mês-AAAA	Nome do responsável pelo teste
Cliente	*Projeto*	
Empresa X	Pentest – target a ser testado	



Anexo Orcamento 01.pdf (0164231) SEI 19.09.02684.0011790/2021-22 / pg. 55

stefaninirafael

Documento	*Emitido em*	*Responsável*
Relatório de Pentest – Target a ser testado	DD-Mês-AAAA	Nome do responsável pelo teste
Cliente	*Projeto*	
Empresa X	Pentest – target a ser testado	



Imagem 2 - Evidência de arquivo configuração do arquivo robots

Anexo Orcamento 01.pdf (0164231) SEI 19.09.02684.0011790/2021-22 / pg. 56

stefaninirafael

Documento	Emitido em	Responsável
Relatório de Pentest – Target a ser testado	DD-Mês-AAAA	Nome do responsável pelo teste
Cliente	**Projeto**	
Empresa X	Pentest – target a ser testado	

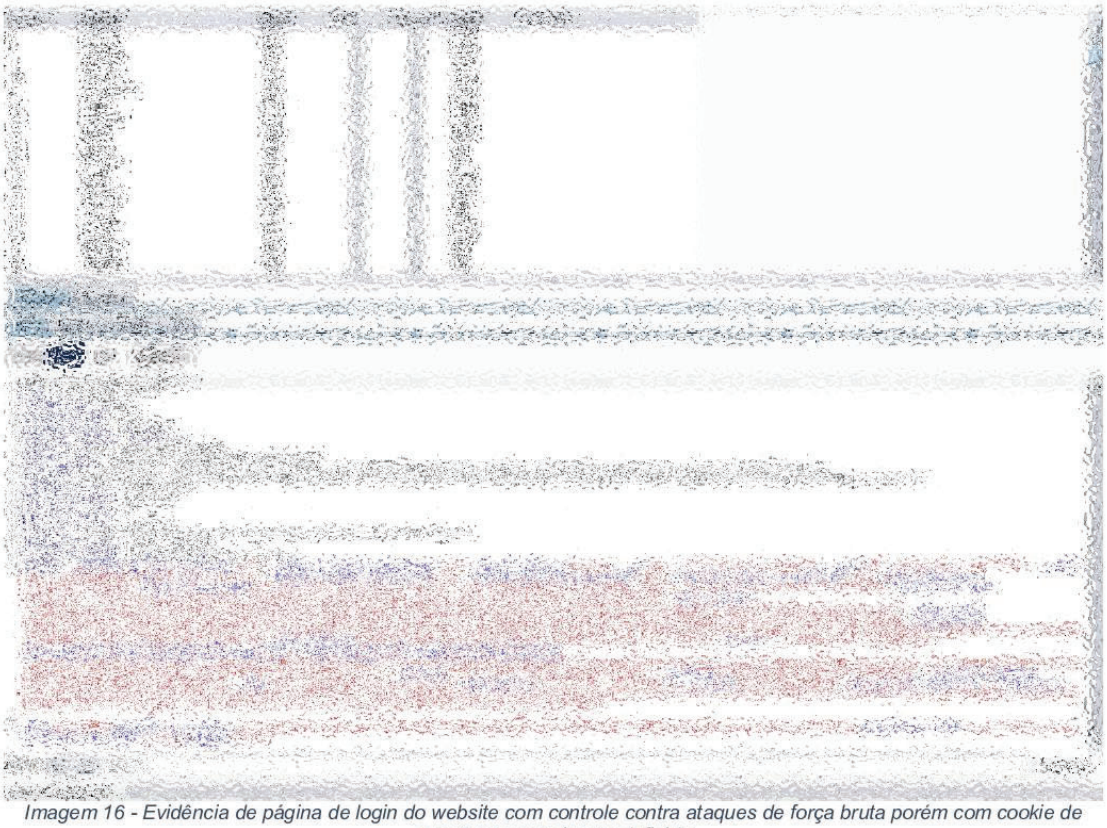


Imagem 16 - Evidência de página de login do website com controle contra ataques de força bruta porém com cookie de sessão sem expiração definida

Anexo Orcamento 01.pdf (0164231) SEI 19.09.02684.0011790/2021-22 / pg. 57

stefaninirafael

Documento	*Emitido em*	*Responsável*
Relatório de Pentest – Target a ser testado	DD-Mês-AAAA	Nome do responsável pelo teste
Cliente	*Projeto*	
Empresa X	Pentest – target a ser testado	



stefaninirafael

Documento	Emitido em	Responsável
Relatório de Pentest – Target a ser testado	DD-Mês-AAAA	Nome do responsável pelo teste
Cliente	**Projeto**	
Empresa X	Pentest – target a ser testado	



Imagem 19 - Evidência de conflitos de chaves SHA1 no código-fonte do aplicativo



Imagem 20 - Evidência de conflitos de chaves SHA1 no código-fonte do aplicativo

Anexo Orcamento 01.pdf (0164231) SEI 19.09.02684.0011790/2021-22 / pg. 59

Voltar Imprimir

CAIXA ECONÔMICA FEDERAL

Certificado de Regularidade do FGTS - CRF

Inscrição: 24.691.488/0001-09
Razão Social: STEFANINI RAFAEL SEGURANCA E DEFESA SA
Endereço: AV EUSEBIO MATOSO 1375 AND 8 SL 801 E 802 / BUTANTA / SAO PAULO / SP / 05423-905

A Caixa Econômica Federal, no uso da atribuição que lhe confere o Art. 7, da Lei 8.036, de 11 de maio de 1990, certifica que, nesta data, a empresa acima identificada encontra-se em situação regular perante o Fundo de Garantia do Tempo de Servico - FGTS.

O presente Certificado não servirá de prova contra cobrança de quaisquer débitos referentes a contribuições e/ou encargos devidos, decorrentes das obrigações com o FGTS.

Validade: 20/04/2021 a 17/08/2021

Certificação Número: 2021042002544302489157

Informação obtida em 17/05/2021 12:50:52

A utilização deste Certificado para os fins previstos em Lei esta condicionada a verificação de autenticidade no site da Caixa: **www.caixa.gov.br**

Anexo Certidão FGTS (0164239) SEI 19.09.02684.0011790/2021-22 / pg. 60

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO

CERTIDÃO NEGATIVA DE DÉBITOS TRABALHISTAS

CNPJ: 24.691.488/0001-09
Certidão nº: 17640021/2021
Expedição: 01/06/2021, às 17:58:20
Validade: 27/11/2021 - 180 (cento e oitenta) dias, contados da data de sua expedição.

Certifica-se que o CNPJ sob o nº **24.691.488/0001-09**, **NÃO CONSTA** do Banco Nacional de Devedores Trabalhistas.
Certidão emitida com base no art. 642-A da Consolidação das Leis do Trabalho, acrescentado pela Lei nº 12.440, de 7 de julho de 2011, e na Resolução Administrativa nº 1470/2011 do Tribunal Superior do Trabalho, de 24 de agosto de 2011.
Os dados constantes desta Certidão são de responsabilidade dos Tribunais do Trabalho e estão atualizados até 2 (dois) dias anteriores à data da sua expedição.
Certidão expedida sem indicação do nome/razão social, tendo em vista que o CPF/CNPJ consultado não figura na última versão da base de dados da Receita Federal do Brasil - RFB enviada ao Tribunal Superior do Trabalho - TST. Para saber a situação desse CPF/CNPJ, consulte o sítio da RFB (www.receita.fazenda.gov.br).
No caso de pessoa jurídica, a Certidão atesta a empresa em relação a todos os seus estabelecimentos, agências ou filiais.
A aceitação desta certidão condiciona-se à verificação de sua autenticidade no portal do Tribunal Superior do Trabalho na Internet (http://www.tst.jus.br).
Certidão emitida gratuitamente.

INFORMAÇÃO IMPORTANTE
Do Banco Nacional de Devedores Trabalhistas constam os dados necessários à identificação das pessoas naturais e jurídicas inadimplentes perante a Justiça do Trabalho quanto às obrigações estabelecidas em sentença condenatória transitada em julgado ou em acordos judiciais trabalhistas, inclusive no concernente aos recolhimentos previdenciários, a honorários, a custas, a emolumentos ou a recolhimentos determinados em lei; ou decorrentes de execução de acordos firmados perante o Ministério Público do Trabalho ou Comissão de Conciliação Prévia.

PREFEITURA DE
SÃO PAULO
FAZENDA

SECRETARIA MUNICIPAL DA FAZENDA

Certidão Conjunta de Débitos de Tributos Mobiliários

Certidão Número: 0662939 - 2021

CPF/CNPJ Raiz: 24.691.488/
Contribuinte: STEFANINI RAFAEL SEGURANCA E DEFESA S.A

Liberação: 28/06/2021
Validade: 26/09/2021

Tributos Abrangidos:

Imposto Sobre Serviços - ISS
Taxa de Fiscalização de Localização Instalação e Funcionamento
Taxa de Fiscalização de Anúncio - TFA
Taxa de Fiscalização de Estabelecimento - TFE
Taxa de Resíduos Sólidos de Serviços de Saúde - TRSS (incidência a partir de Jan/2011)
Imposto Sobre Transmissão de Bens Imóveis - ITBI

Unidades Tributárias:

CCM 5.603.212-9- Inicio atv :17/10/2016 (AV EUSEBIO MATOSO, 1375 - CEP: 05423-180)

Ressalvado o direito de a Fazenda Municipal cobrar e inscrever quaisquer dívidas de responsabilidade do sujeito passivo que vierem a ser apuradas ou que se verifiquem a qualquer tempo, inclusive em relação ao período contido neste documento, relativas a tributos administrados pela Secretaria Municipal da Fazenda e a inscrições em Dívida Ativa Municipal, junto à Procuradoria Geral do Município é certificado que a Situação Fiscal do Contribuinte supra, referente aos créditos tributários inscritos e não inscritos na Dívida Ativa abrangidos por esta certidão, até a presente data é: **REGULAR.**

A aceitação desta certidão está condicionada à verificação de sua autenticidade na Internet, no endereço http://www.prefeitura.sp.gov.br/cidade/secretarias/fazenda/.
Qualquer rasura invalidará este documento.

SITUAÇÃO REGULAR

Certidão expedida com base na Portaria Conjunta SF/PGM nº 4, de 12 de abril de 2017, Instrução Normativa SF/SUREM nº 3, de 6 de abril de 2015, Decreto 50.691, de 29 de junho de 2009, Decreto 51.714, de 13 de agosto de 2010 e Portaria SF nº 268, de 11 de outubro de 2019.

Certidão emitida às 10:25:25 horas do dia 26/07/2021 (hora e data de Brasília).

Código de Autenticidade: 8C29245D

A autenticidade desta certidão deverá ser confirmada na página da Secretaria Municipal da Fazenda http://www.prefeitura.sp.gov.br/sf

Secretaria da Fazenda e Planejamento do Estado de São Paulo

Débitos Tributários Não Inscritos na Dívida Ativa do Estado de São Paulo

CNPJ / IE: 24.691.488/0001-09

Ressalvado o direito da Secretaria da Fazenda e Planejamento do Estado de São Paulo de apurar débitos de responsabilidade da pessoa jurídica acima identificada, é certificado que **não constam débitos** declarados ou apurados pendentes de inscrição na Dívida Ativa de responsabilidade do estabelecimento matriz/filial acima identificado.

Certidão nº	21060013034-58
Data e hora da emissão	01/06/2021 17:36:57
Validade	6 (seis) meses, contados da data de sua expedição.

Qualquer rasura ou emenda invalidará este documento.

A aceitação desta certidão está condicionada à verificação de sua autenticidade no sítio **www.pfe.fazenda.sp.gov.br**

MINISTÉRIO DA FAZENDA
Secretaria da Receita Federal do Brasil
Procuradoria-Geral da Fazenda Nacional

CERTIDÃO NEGATIVA DE DÉBITOS RELATIVOS AOS TRIBUTOS FEDERAIS E À DÍVIDA ATIVA DA UNIÃO

Nome: STEFANINI RAFAEL SEGURANCA E DEFESA S.A.
CNPJ: 24.691.488/0001-09

Ressalvado o direito de a Fazenda Nacional cobrar e inscrever quaisquer dívidas de responsabilidade do sujeito passivo acima identificado que vierem a ser apuradas, é certificado que não constam pendências em seu nome, relativas a créditos tributários administrados pela Secretaria da Receita Federal do Brasil (RFB) e a inscrições em Dívida Ativa da União (DAU) junto à Procuradoria-Geral da Fazenda Nacional (PGFN).

Esta certidão é válida para o estabelecimento matriz e suas filiais e, no caso de ente federativo, para todos os órgãos e fundos públicos da administração direta a ele vinculados. Refere-se à situação do sujeito passivo no âmbito da RFB e da PGFN e abrange inclusive as contribuições sociais previstas nas alíneas 'a' a 'd' do parágrafo único do art. 11 da Lei nº 8.212, de 24 de julho de 1991.

A aceitação desta certidão está condicionada à verificação de sua autenticidade na Internet, nos endereços <http://rfb.gov.br> ou <http://www.pgfn.gov.br>.

Certidão emitida gratuitamente com base na Portaria Conjunta RFB/PGFN nº 1.751, de 2/10/2014.
Emitida às 17:53:13 do dia 01/06/2021 <hora e data de Brasília>.
Válida até 28/11/2021.
Código de controle da certidão: **6D7A.67A0.05D3.E6A0**
Qualquer rasura ou emenda invalidará este documento.

Anexo Certidao Federal (0164253) SEI 19.09.02684.0011790/2021-22 / pg. 64

REPÚBLICA FEDERATIVA DO BRASIL

CADASTRO NACIONAL DA PESSOA JURÍDICA

NÚMERO DE INSCRIÇÃO	COMPROVANTE DE INSCRIÇÃO E DE SITUAÇÃO CADASTRAL	DATA DE ABERTURA
24.691.488/0001-09 **MATRIZ**		**29/04/2016**

NOME EMPRESARIAL
STEFANINI RAFAEL SEGURANCA E DEFESA S.A.

TÍTULO DO ESTABELECIMENTO (NOME DE FANTASIA)	PORTE
********	**DEMAIS**

CÓDIGO E DESCRIÇÃO DA ATIVIDADE ECONÔMICA PRINCIPAL
62.03-1-00 - Desenvolvimento e licenciamento de programas de computador não-customizáveis

CÓDIGO E DESCRIÇÃO DAS ATIVIDADES ECONÔMICAS SECUNDÁRIAS
62.01-5-01 - Desenvolvimento de programas de computador sob encomenda
62.02-3-00 - Desenvolvimento e licenciamento de programas de computador customizáveis
62.09-1-00 - Suporte técnico, manutenção e outros serviços em tecnologia da informação
62.04-0-00 - Consultoria em tecnologia da informação
95.11-8-00 - Reparação e manutenção de computadores e de equipamentos periféricos
46.51-6-01 - Comércio atacadista de equipamentos de informática
64.62-0-00 - Holdings de instituições não-financeiras

CÓDIGO E DESCRIÇÃO DA NATUREZA JURÍDICA
205-4 - Sociedade Anônima Fechada

LOGRADOURO	NÚMERO	COMPLEMENTO
AV EUSEBIO MATOSO 1375	**1375**	**ANDAR 8 SALA 801 E 802**

CEP	BAIRRO/DISTRITO	MUNICÍPIO	UF
05.423-905	**BUTANTA**	**SAO PAULO**	**SP**

ENDEREÇO ELETRÔNICO	TELEFONE
GESTAOTRIBUTARIA@STEFANINI.COM	**(11) 3094-6174**

ENTE FEDERATIVO RESPONSÁVEL (EFR)
*****

SITUAÇÃO CADASTRAL	DATA DA SITUAÇÃO CADASTRAL
ATIVA	**29/04/2016**

MOTIVO DE SITUAÇÃO CADASTRAL

SITUAÇÃO ESPECIAL	DATA DA SITUAÇÃO ESPECIAL
********	********

Aprovado pela Instrução Normativa RFB nº 1.863, de 27 de dezembro de 2018.

Emitido no dia **25/05/2021** às **19:59:59** (data e hora de Brasília). Página: **1/1**

Anexo Cadastro Pessoa Juridica (0164260) SEI 19.09.02684.0011790/2021-22 / pg. 65

Prefeitura da Cidade de São Paulo

Auto de Licença de Funcionamento

DADOS DA LICENÇA

NÚMERO: 20190010044559 DATA DE EMISSÃO: 05/09/2019 DATA DE VALIDADE: Indeterminada

DADOS DO CADASTRO DO IMÓVEL

ENDEREÇO: AV EUSEBIO MATOSO 1375, 1375

BAIRRO: BUTANTA CEP: 05423-905 CIDADE-UF: SÃO PAULO - SP

SUBPREFEITURA: BUTANTA ÁREA CONSTRUÍDA: 887,00 m² ÁREA ESTABELECIMENTO: 500,00 m²

SQL: 200.055.0025-5 (Principal)

ZONA(S):

ZM - ZONA MISTA

DADOS DA EMPRESA / ESTABELECIMENTO

CNPJ: 24.691.488/0001-09 REGISTRO: 35300492650 CCM: 5.603.212-9

RAZÃO SOCIAL: STEFANINI RAFAEL SEGURANÇA E DEFESA S.A

ATIVIDADES

CNAE: 6203-1/00 - Desenvolvimento e licenciamento de programas de computador não-customizáveis Versão CNAE: 2.3 RISCO: BAIXO

GRUPO DE ATIVIDADE NR:

nR1-6: Serviços profissionais: estabelecimentos destinados à prestação de serviços de profissionais liberais, técnicos ou universitários ou de residencial;apoio ao uso residencial;

ATIVIDADE(S):

Escritórios em geral, incluindo espaços para Locação de Uso Compartilhado e "Co-Working"

RESPONSÁVEL PELA SOLICITAÇÃO DE LICENCIAMENTO

RESPONSÁVEL PELO PEDIDO: MARCO ANTONIO SILVA STEFANINI CPF: 042.501.968-36

PROCESSO ADMINISTRATIVO: 6031.2019/0003603-2

AUTENTICIDADE

CNPJ: 24.691.488/0001-09 NÚMERO DA LICENÇA: 20190010044559 CÓDIGO DE AUTENTICIDADE: HRYhaT6Nd9oWYDDF

LICENÇA:

Anexo Álvara de Funcionamento (0164264) SEI 19.09.02684.0011790/2021-22 / pg. 66

ANÁLISE DE VIABILIDADE

CNAE: 6203-1/00 **STATUS DA ANÁLISE:** Passível **DATA DA ANÁLISE:** 04/09/2019

RESTRIÇÕES:

Grupo de Atividade [nR1-6: Serviços profissionais: estabelecimentos destinados à prestação de serviços de profissionais liberais, técnicos ou universitários ou de residencial;apoio ao uso residencial;] PASSÍVEL: Permitida a instalação da atividade no imóvel em questão em função da zona de uso.

Grupo de Atividade [nR3-1: Usos especiais: espaços, estabelecimentos ou instalações sujeitos a controle específico ou de valor estratégico para a segurança e serviços públicos;] PASSÍVEL: Permitida a instalação da atividade no imóvel em questão em função da zona de uso.

Quadro 4B - Parâmetros de incomodidade por zona : Zona [ZM]: Nível Critério de Avaliação (NCA) para ambiente externo dB(A) (c) (d) (f): Emissão ruído 7h-19h = Emissão máxima de 60 dB 4B(c) No caso dos aeroportos aplica-se o nível de ruído conforme norma técnica específica. 4B(d) Poderão incidir parâmetros especiais e mais restritivos nos termos §2º do artigo 113 desta lei. 4B(f) Para atividade de local de culto, nos feriados, sábados a partir das 14h e nos domingos, os parâmetros relativos a ruídos referentes ao período das 7h às 19h passam a valer também para os períodos das 6h às 7h e das 19h às 22h, permanecendo inalterados os parâmetros referentes ao período das 7h às 19h e das 22h às 7h.

Quadro 4B - Parâmetros de incomodidade por zona : Zona [ZM]: Nível Critério de Avaliação (NCA) para ambiente externo dB(A) (c) (d) (f): Emissão ruído 19h-22h = Emissão máxima de 55 dB 4B(c) No caso dos aeroportos aplica-se o nível de ruído conforme norma técnica específica. 4B(d) Poderão incidir parâmetros especiais e mais restritivos nos termos §2º do artigo 113 desta lei. 4B(f) Para atividade de local de culto, nos feriados, sábados a partir das 14h e nos domingos, os parâmetros relativos a ruídos referentes ao período das 7h às 19h passam a valer também para os períodos das 6h às 7h e das 19h às 22h, permanecendo inalterados os parâmetros referentes ao período das 7h às 19h e das 22h às 7h.

Quadro 4B - Parâmetros de incomodidade por zona : Zona [ZM]: Nível Critério de Avaliação (NCA) para ambiente externo dB(A) (c) (d) (f): Emissão ruído 22h-7h = Emissão máxima de 50 dB 4B(c) No caso dos aeroportos aplica-se o nível de ruído conforme norma técnica específica. 4B(d) Poderão incidir parâmetros especiais e mais restritivos nos termos §2º do artigo 113 desta lei. 4B(f) Para atividade de local de culto, nos feriados, sábados a partir das 14h e nos domingos, os parâmetros relativos a ruídos referentes ao período das 7h às 19h passam a valer também para os períodos das 6h às 7h e das 19h às 22h, permanecendo inalterados os parâmetros referentes ao período das 7h às 19h e das 22h às 7h.

Quadro 4B - Parâmetros de incomodidade por zona : Zona [ZM]: Vibração associada = 4B(a) 4B(a) Aplicam-se a legislação pertinente e as normas técnicas brasileiras - ABNT em vigor.

Quadro 4B - Parâmetros de incomodidade por zona : Zona [ZM]: Emissão de odores = 4B(a) 4B(a) Aplicam-se a legislação pertinente e as normas técnicas brasileiras - ABNT em vigor.

Quadro 4B - Parâmetros de incomodidade por zona : Zona [ZM]: Emissão de gases, vapores e material particulado (e) = 4B(a) 4B(a) Aplicam-se a legislação pertinente e as normas técnicas brasileiras - ABNT em vigor. 4B(e) Quando necessário a CETESB recomenda instalar e operar sistema de controle de poluição do ar baseado na melhor tecnologia.

Quadro 4B - Parâmetros de incomodidade por zona : Zona [ZM]: Emissão de radiação Faixa de frequência (0Hz à 300GHz) = 4B(b) 4B(b) Aplicam-se a legislação pertinente e as normas técnicas em vigor, sendo que o Executivo poderá estabelecer parâmetros mais restritivos de radiação eletromagnéticas não ionizantes.

Quadro 4A - Condições de instalação por subcategoria de uso, grupos de atividade e usos específicos : Grupo de Atividade [nR3-1]: Número mínimo de vagas por área construída computável (em m²) ou por número de unidades habitacionais (UH) (a): Vagas de automóveis (e)(f) = Mínimo de 1 vaga a cada 75 m² de área construída computável Obs: 4A(a) Não se aplica nas zonas de uso ZEU, ZEUa, ZEUP, ZEUPa, ZEM, ZEMP e nos usos não residenciais em lotes com área inferior a 250m² (duzentos e cinquenta metros quadrados) em todas as zonas. 4A(e) Para Serviços de Armazenamento e Guarda de Bens Móveis das subcategorias de uso nR1, nR2 e nR3, o número mínimo de vagas de automóveis exigido será calculado com base na área construída computável destinada à permanência humana. 4A(f) Quando exigido o número mínimo de vagas de automóveis, este deverá ser acrescido do número de vagas especiais conforme definido no Código de Obras e Edificações.

Quadro 4A - Condições de instalação por subcategoria de uso, grupos de atividade e usos específicos : Grupo de Atividade [nR3-1]: Número mínimo de vagas por área construída computável (em m²) ou por número de unidades habitacionais (UH) (a): Vagas de bicicletas = Mínimo de 1 vaga a cada 500 m² de área construída computável Obs: 4A(a) Não se aplica nas zonas de uso ZEU, ZEUa, ZEUP, ZEUPa, ZEM, ZEMP e nos usos não residenciais em lotes com área inferior a 250m² (duzentos e cinquenta metros quadrados) em todas as zonas.

Quadro 4A - Condições de instalação por subcategoria de uso, grupos de atividade e usos específicos : Grupo de Atividade [nR3-1]: Vestiário para usuários de bicicleta (b) = Se aplica essa condição de instalação Obs: 4A(b) De acordo com o Código de Obras e Edificações.

Quadro 4A - Condições de instalação por subcategoria de uso, grupos de atividade e usos específicos : Grupo de Atividade [nR3-1]: Espaço para carga e descarga (c): Número de vagas para utilitário = Mínimo de 1 vaga e 1 vaga adicional a cada 4.000 m² de área construída computável Obs: 4A(c) Não se exige vaga para carga e descarga nos lotes com área até 250m² (duzentos e cinquenta metros quadrados), exceto em lotes localizados na Macroárea de Urbanização Consolidada e nos seguintes setores e subsetores da Macroárea de Estruturação Metropolitana: I. Subsetores Arco Tietê, Arco Pinheiros e Arco Faria Lima - Águas Espraiadas - Chucri Zaidan do Setor Orla Ferroviária e Fluvial. II. Setor Central (Operação Urbana Centro).

Anexo Álvara de Funcionamento (0164264) SEI 19.09.02684.0011790/2021-22 / pg. 67

Quadro 4A - Condições de instalação por subcategoria de uso, grupos de atividade e usos específicos : Grupo de Atividade [nR3-1]: Espaço para carga e descarga (c): Número de vagas para caminhão: Acima de 4.000m² de área construída computável (d) = Não há exigência de número mínimo de vagas Obs: 4A(c) Não se exige vaga para carga e descarga nos lotes com área até 250m² (duzentos e cinquenta metros quadrados), exceto em lotes localizados na Macroárea de Urbanização Consolidada e nos seguintes setores e subsetores da Macroárea de Estruturação Metropolitana: I. Subsetores Arco Tietê, Arco Pinheiros e Arco Faria Lima - Águas Espraiadas - Chucri Zaidan do Setor Orla Ferroviária e Fluvial. II. Setor Central (Operação Urbana Centro). 4A(d) Para empreendimentos não residenciais acima de 10.000m² (dez mil metros quadrados) de área construída computável, as vagas para caminhão podem ser compartilhadas com os veículos fretados.

Imóvel informado está inserido na Macroárea de Estruturação Metropolitana - MEM. Verificar a existência de lei específica para a região informada, nos termos do §3º do art. 76 da Lei nº 16.050/14.

Ao continuar o processo, você assume a responsabilidade pelo endereço e inscrição imobiliária informados, ciente de que o resultado pode ser revertido caso seja apurada incorreção dos mesmos, sem prejuízo das demais penas da lei

Atividade passível de instalação no local, conforme disposições da legislação urbanística municipal em vigor.

GRUPO DE ATIVIDADE NR: nR1-6 **STATUS DA ANÁLISE:** Passível

RESTRIÇÕES:

Quadro 4A - Condições de instalação por subcategoria de uso, grupos de atividade e usos específicos : Grupo de Atividade [nR1-6]: Número mínimo de vagas por área construída computável (em m²) ou por número de unidades habitacionais (UH) (a): Vagas de automóveis (e)(f) = Mínimo de 1 vaga a cada 75 m² de área construída computável Obs: 4A(a) Não se aplica nas zonas de uso ZEU, ZEUa, ZEUP, ZEUPa, ZEM, ZEMP e nos usos não residenciais em lotes com área inferior a 250m² (duzentos e cinquenta metros quadrados) em todas as zonas. 4A(e) Para Serviços de Armazenamento e Guarda de Bens Móveis das subcategorias de uso nR1, nR2 e nR3, o número mínimo de vagas de automóveis exigido será calculado com base na área construída computável destinada à permanência humana. 4A(f) Quando exigido o número mínimo de vagas de automóveis, este deverá ser acrescido do número de vagas especiais conforme definido no Código de Obras e Edificações.

Quadro 4A - Condições de instalação por subcategoria de uso, grupos de atividade e usos específicos : Grupo de Atividade [nR1-6]: Número mínimo de vagas por área construída computável (em m²) ou por número de unidades habitacionais (UH) (a): Vagas de bicicletas = Mínimo de 1 vaga a cada 250 m² de área construída computável Obs: 4A(a) Não se aplica nas zonas de uso ZEU, ZEUa, ZEUP, ZEUPa, ZEM, ZEMP e nos usos não residenciais em lotes com área inferior a 250m² (duzentos e cinquenta metros quadrados) em todas as zonas.

Quadro 4A - Condições de instalação por subcategoria de uso, grupos de atividade e usos específicos : Grupo de Atividade [nR1-6]: Espaço para carga e descarga (c): Número de vagas para utilitário = Mínimo de 1 vaga e 1 vaga adicional a cada 4.000 m² de área construída computável Obs: 4A(c) Não se exige vaga para carga e descarga nos lotes com área até 250m² (duzentos e cinquenta metros quadrados), exceto em lotes localizados na Macroárea de Urbanização Consolidada e nos seguintes setores e subsetores da Macroárea de Estruturação Metropolitana: I. Subsetores Arco Tietê, Arco Pinheiros e Arco Faria Lima - Águas Espraiadas - Chucri Zaidan do Setor Orla Ferroviária e Fluvial. II. Setor Central (Operação Urbana Centro).

DETALHAMENTO

A Prefeitura de São Paulo expede o presente Auto de Licença de Funcionamento para empreendimentos de baixo risco, nos termos do Decreto Municipal 57.299/2016, devendo ainda serem observadas as legislações estadual e federal pertinentes.

DECLARAÇÕES:

Declaro, sob as penas da Lei: - que os dados informados neste formulário e os dados relativos à edificação são verdadeiros, não havendo impedimentos de terceiros, e de qualquer ordem, no tocante a sua utilização, e que a inexatidão, irregularidade ou falsidade na prestação das informações relativas ao licenciamento eletrônico sujeitará o responsável, juntamente com as demais pessoas que derem causa, às penalidades administrativas, civis e criminais cabíveis; - que a atividade atende às exigências legais, gerais e especiais, relativas ao seu exercício, e que o simples protocolo do pedido de licença por qualquer meio não autoriza o funcionamento da atividade, nos termos do art. 18 do Decreto Municipal nº 57.299/16; - estar ciente de que a Prefeitura do Município de São Paulo não se responsabiliza por requerimentos via Internet não recebidos por motivo de ordem técnica dos computadores, falhas de comunicação, congestionamento das linhas de comunicação ou outros fatores de ordem técnica que impossibilitem a transferência de dados, bem como informações de endereço incorretas, incompletas ou por falha na entrega de mensagens eletrônicas causadas por endereço eletrônico incorreto ou por problemas do provedor de acesso do requerente.

Declaro estar ciente que a obtenção do Auto de Licença de Funcionamento para empreendimentos de baixo risco não substitui as demais licenças e autorizações necessárias e não substitui qualquer documento expedido pela PMSP relativo à regularidade da edificação.

Declaro que o estabelecimento atende todos os requisitos legais, dentre os quais aqueles relacionados à manipulação de materiais tóxicos, explosivos e que possam causar algum tipo de contaminação, nos termos do art 4° do Decreto Municipal nº 57.298/2016, bem como atende aos requisitos legais nos casos de atividades em imóveis em que sejam armazenados ou utilizados líquidos combustíveis.

Declaro que, caso o estabelecimento seja ocupado por mais de uma atividade não residencial, e, não seja possível diferenciar os parâmetros aplicáveis a cada uso, serão atendidas as condições de instalação da atividade mais restritiva, nos termos do §2º do art. 112 da Lei Municipal nº 16.402/2016 e que, caso ocorram alterações referentes ao tipo ou características da atividade, do Cadastro de Contribuintes Imobiliários - CCM, da razão social do estabelecimento - CNPJ, ou quando houver modificações na edificação utilizada ou por exigência legal, o Auto de Licença de Funcionamento deverá, obrigatoriamente, ser renovado, nos termos da Lei Municipal nº 10.205/1986.

Anexo Álvara de Funcionamento (0164264) SEI 19.09.02684.0011790/2021-22 / pg. 68

Declaro que a(s) cópia(s) digitalizada(s) da(s) Anotação(ções) de Responsabilidade Técnica (ART(s)) ou do(s) Registro(s) de Responsabilidade Técnica (RRT(s)) anexada(s) ao sistema e emitida(s) em conformidade com as exigências dos órgãos de classe refere(m)-se ao estabelecimento no qual se pretende instalar a atividade, conforme descrito no Decreto nº 57.299/2016.

Declaro que, caso o empreendimento esteja instalado em edificação não regular de acordo com as definições da legislação edilícia, serão asseguradas as condições de higiene, segurança de uso, estabilidade, habitabilidade da edificação, assim como as condições de instalação e os parâmetros de incomodidade, conforme disposto no Art. 133 da Lei Municipal nº 16.402/2016. Declaro ainda que o imóvel não está situado em non aedificandi, de risco geológico-geotécnico ou de preservação ambiental permanente, e que a edificação não invade logradouro ou terreno público, nem tampouco é objeto de ação judicial promovida pelo Município de São Paulo, objetivando a sua demolição.

Declaro que mantenho em meu poder e à disposição da fiscalização, a Anotação de Responsabilidade Técnica (ART) ou Registro de Responsabilidade Técnica (RRT), anexadas a esta solicitação, bem como a cópia da carteira do responsável técnico no Conselho de Classe, que atestam as condições de segurança, acessibilidade, habitabilidade, salubridade, equipamentos e instalações prediais, elétricas e de gás da edificação, e que o imóvel se encontra estável, inclusive com relação a coberturas, nos termos dos incisos II e III do Art. 12 do Decreto Municipal nº 57.299/2016, e em satisfatórias condições de segurança, e que, com base na legislação edilícia, nos casos em que há obrigatoriedade do sistema de segurança, o controle da manutenção do referido sistema será realizado de acordo com as normas técnicas em vigor e possuo os respectivos documentos municipais comprobatórios das condições de segurança e acessibilidade.

Declaro que estou ciente que não é permitida a utilização das edificações para usos não residenciais quando o lote resultante de aprovação de empreendimentos enquadrados na subcategoria de uso R2h-1 (casas geminadas) não atender às dimensões e a área mínimas do Quadro 2A da Lei Municipal nº 16.402/2016, conforme art. 16 do Decreto Municipal nº 57.521/2016.

Declaro que, caso a atividade esteja enquadrado como atividade auxiliar da subcategoria de uso INFRA-1 - Mobilidade urbana terrestre ou INFRA-2 - Transporte aéreo, ou seja, atividade instalada em áreas que servem ao transporte público coletivo ou ao transporte aéreo, respectivamente, atendo às condições previstas no art. 7º do Decreto Municipal nº 57.378/2016, inclusive quanto à obtenção de avaliação técnica favorável do órgão gestor do empreendimento.

Declaro que, caso o estabelecimento tenha utilizado benefícios estabelecidos em legislação específica para a atividade declarada, esta está em acordo com as exigências previstas no momento da aprovação do projeto.

Declaro que o conhecimento e a concordância das demais declarações não exime da observância da legislação pertinente ao tema, assim como dos procedimentos e penalidades decorrentes de seu não atendimento, e que estou ciente que o Auto de Licença deverá ser afixado permanentemente no acesso principal do estabelecimento, em posição visível para o público, conforme disposto no Art. 140 da Lei Municipal nº 16.402/2016.

Declaro que o estabelecimento não possui 120 (cento e vinte) vagas de estacionamento ou mais e está localizado em Área Especial de Tráfego (AET) ou 280 (duzentas e oitenta) vagas de estacionamento ou mais, localizado nas demais áreas do Município, nos termos dos art. 108 e 109 da Lei Municipal nº 16.402/16.

Declaro que o empreendimento é permanente e não atrai ou produz grande número de viagens ao longo do dia e/ou por período determinado, causando impacto no sistema viário e de transporte, podendo comprometer a acessibilidade, a mobilidade e a segurança de veículos e pedestres, nos termos da dos art. 108 e 109 da Lei Municipal nº 16.402/16.

Declaro que o estabelecimento não se enquadra como atividade secundária ou complementar, nos termos do art. 33 do Decreto Municipal nº 49.969/08.

Declaro que o estabelecimento no qual se pretende instalar a atividade não é atividade enquadrada como Empreendimento Gerador de Impacto de Vizinhança ou como Empreendimento Gerador de Impacto Ambiental, nos termos do art. 108 da Lei Municipal nº 16.402/16.

Declaro que o estabelecimento no qual pretendo instalar a atividade não está sujeito a controle específico e não é de valor estratégico para a segurança e serviços públicos, nos termos da Lei Municipal nº 16.402/16 e do Decreto Municipal nº 57.378/16.

CONDIÇÕES:

Emitido eletronicamente

COORDENADORIA DE VIGILÂNCIA EM SAÚDE - COVISA - SECRETARIA MUNICIPAL DE SAÚDE – SMS: Esta atividade é válida para todos os fins legais e está dispensada da licença da Coordenadoria de Vigilância em Saúde - COVISA, vinculada à Secretaria Municipal da Saúde.

DEPARTAMENTO DE CONTROLE DE QUALIDADE AMBIENTAL-2 / GRUPO TÉCNICO DE AVALIAÇÃO DE IMPACTO AMBIENTAL DE ATIVIDADES INDUSTRIAIS (GTAIA-IND) SECRETARIA MUNICIPAL DO VERDE E MEIO AMBIENTE - SVMA: Esta atividade está dispensada da licença ambiental gerida pelo Departamento de Controle da Qualidade Ambiental - DECONT, vinculado à Secretaria do Verde e do Meio Ambiente - SVMA. Entretanto, a atividade poderá estar sujeita ao licenciamento pelo órgão ambiental competente, e por tal questão esta licença municipal não exclui a obrigatoriedade de obter a licença junto a Companhia de Tecnologia de Saneamento Ambiental (CETESB).

JUCESP
29 04 16

INSTRUMENTO PARTICULAR DE CONSTITUIÇÃO DA
SOCIEDADE EMPRESÁRIA LIMITADA
"STF PROJETOS E SERVIÇOS DE TECNOLOGIA DE DEFESA LTDA."

Pelo presente instrumento particular e na melhor forma de direito, as partes abaixo:

1. **STEFANINI PARTICIPAÇÕES S.A.**, sociedade empresária limitada, com sede na Calçada das Margaridas, n.º.163, sala 2, Centro Comercial de Alphaville, Cidade de Barueri, Estado de São Paulo, CEP 06453-038, devidamente inscrita no CNPJ/MF sob o nº 04.300.049/0001-10, com seus atos constitutivos devidamente registrados perante a Junta Comercial do Estado de São Paulo, sob o NIRE 35300490673, em sessão do dia 07 de maio de 2004, neste ato representada na forma de seu contrato social, por sua Diretora, **Marias das Graças Vuolo Sajovic Stefanini**, abaixo qualificado; e

2. **MARCO ANTÔNIO SILVA STEFANINI**, brasileiro, casado sob o regime de comunhão universal de bens, empresário e geólogo, portador da Cédula de Identidade RG nº.10.153.181-3 SSP/SP, e do CPF nº. 042.501.968-36, residente e domiciliado na Praça dos Carvalhos, L14, Condomínio Duas Marias, na cidade de Jaguariúna, Estado de São Paulo, CEP 13820-000,

têm entre si justo e contratado constituir uma sociedade empresária limitada, nos termos dos arts. 966 e 982 e do art. 1052 e seguintes do Código Civil, que se regerá pelas seguintes cláusulas e condições, que mutuamente outorgam e aceitam, a saber:

"CONTRATO SOCIAL DA
STF PROJETOS E SERVIÇOS DE TECNOLOGIA DE DEFESA LTDA.

CAPÍTULO I
Denominação, Lei Aplicável, Sede, Foro e Prazo de Duração

ARTIGO 1º A sociedade empresária limitada opera sob a denominação de **STF PROJETOS E SERVIÇOS DE TECNOLOGIA DE DEFESA LTDA.** e rege-se pelo presente Contrato Social, pelas disposições legais aplicáveis às sociedades empresárias limitadas, nos termos dos arts. 966 e 982 e do art. 1052 e seguintes do Código Civil, e, supletivamente, pela Lei das Sociedades por Ações.

ARTIGO 2º A sociedade tem sede e foro jurídico na Avenida Marginal, 156, sala 3, Centro, na Cidade de Jaguariúna, Estado de São Paulo, CEP 13.820-000.

PARÁGRAFO ÚNICO - A sociedade poderá, por deliberação dos sócios, abrir, transferir ou encerrar filiais no Brasil ou no exterior.

ARTIGO 3º A sociedade tem prazo de duração indeterminado.

CAPÍTULO II
Objeto Social

ARTIGO 4º A sociedade tem por objeto (i) a prestação de serviços de tecnologia industrial básica, projetos, pesquisa, desenvolvimento e inovação tecnológicos, assistência técnica, consultoria e transferência de tecnologia de defesa, incluindo serviços técnicos especializados de defesa cibernética; (ii) o desenvolvimento de soluções de automação industrial, suporte técnico de informática e sistemas de defesa e de inteligência, incluindo atividades de comando e controle cibernéticos; (iii) o

JUCESP
29 04 16

licenciamento e desenvolvimento de software próprio ou de terceiros de defesa; e (iv) a participação em outras sociedades de qualquer tipo societário, como sócia ou acionista.

CAPÍTULO III
Capital Social

ARTIGO 5º O capital social, totalmente subscrito e integralizado em moeda corrente nacional, é de R$ 1.000,00 (um mil reais), dividido em 1.000 (mil) quotas, do valor nominal de R$ 1,00 (um real) cada uma, assim distribuídas aos sócios:

SÓCIOS	Nº DE QUOTAS DETIDAS	VALOR NOMINAL (R$)
STEFANINI PARTICIPAÇÕES LTDA.	999	999,00
MARCO ANTÔNIO SILVA STEFANINI	1	1,00
TOTAL	1.000	1.000,00

PARÁGRAFO ÚNICO - A responsabilidade de cada sócio é, na forma da lei, restrita ao valor de suas quotas, mas ambos respondem solidariamente pela integralização do capital social.

ARTIGO 6º As quotas são indivisíveis em relação à sociedade e cada quota confere ao seu titular o direito a um voto nas deliberações dos sócios.

PARÁGRAFO ÚNICO - Exceto se de outra forma exigido por lei ou disposto neste Contrato Social, as deliberações dos sócios serão tomadas pelo(s) sócio(s) representando a maioria do capital social, inclusive a que dispuser sobre a transformação da sociedade em outro tipo societário.

ARTIGO 7º A transferência ou a alienação, no todo ou em parte, de quotas do capital social a terceiros não será permitida sem o consentimento prévio, por escrito, do(s) sócio(s) representando a maioria do capital social, a qual terá direito de preferência para sua aquisição pelo mesmo preço e condições constantes da oferta formulada, por escrito, por terceiros.

CAPÍTULO IV
Administração

ARTIGO 8º A sociedade poderá ser administrada por sócios ou não, desde que residentes no País. A sociedade será administrada exclusiva e individualmente pela administradora **MARIA DAS GRAÇAS VUOLO SAJOVIC STEFANINI**, brasileira, casada, empresária, portadora da cédula de identidade RG nº 8.546.223-8 SSP/SP e inscrita no CPF/MF sob o nº 015.819.138-26, residente e domiciliada na cidade de Jaguariúna, Estado de São Paulo, na Praça dos Carvalhos, L14, Condomínio Duas Marias, CEP 13820-000, designada **Diretora**.

PARÁGRAFO ÚNICO – O Diretor permanecerá em seu cargo por prazo indeterminado, até que venha a ser destituído e/ou substituído por deliberação do(s) sócio(s) representando, no mínimo, o quorum exigido por lei.

ARTIGO 9º O Diretor terá poderes para administrar e gerir os negócios sociais e

Anexo Contrato Social (0165188) SEI 19.09.02684.0011790/2021-22 / pg. 71

JUCESP
29 04 16

para, agindo individualmente, representar e obrigar a sociedade para todos os fins.

PARÁGRAFO ÚNICO - A sociedade poderá, ainda, ser representada por procuradores, de acordo com a extensão dos poderes contidos nos respectivos instrumentos de mandato.

ARTIGO 10 Quaisquer atos praticados pelo Diretor, por procuradores ou por funcionários da sociedade, envolvendo obrigações relacionadas com negócios e operações estranhos ao objeto social, tais como o fornecimento de fianças, avais ou quaisquer garantias em favor de terceiros, são expressamente proibidos e serão nulos de pleno direito, exceto se expressamente autorizados, por escrito, por sócio(s) representando a maioria do capital social.

CAPÍTULO V
Reuniões dos sócios

ARTIGO 11 Os sócios reunir-se-ão sempre que os interesses sociais assim o exigirem. Entretanto, qualquer deliberação que demandar a manifestação dos sócios poderá ser tida como validamente tomada, independentemente de realização de reunião, se expressa mediante instrumento escrito, firmado por sócio(s) representando a totalidade do capital social.

PARÁGRAFO 1º - As reuniões dos sócios serão convocadas por qualquer uma dos sócios ou por Diretores, através de carta registrada, fax ou aviso entregue pessoalmente, contra recibo, a ambos os sócios, com a antecedência, mínima, de 8 (oito) dias. Considerar-se-á dispensada a convocação quando os sócios comparecerem à reunião ou se declararem, por escrito, cientes do local, data, hora e Ordem do Dia.

PARÁGRAFO 2º - As reuniões dos sócios serão instaladas com a presença de titular(es) de quotas representando, no mínimo, 75% (setenta e cinco por cento) do capital social, em primeira convocação, e a maioria do capital social, em segunda convocação, e serão presididas e secretariadas por Presidente e Secretário escolhidos pelo(s) sócio(s) presente(s).

PARÁGRAFO 3º - Qualquer sócio poderá fazer-se representar nas reuniões dos sócios por outro sócio ou por advogado, mediante outorga de procuração, com especificação dos atos autorizados, devendo a procuração ser levada a registro juntamente com a ata.

PARÁGRAFO 4º - A sociedade manterá um livro de atas das reuniões dos sócios, no qual as atas das reuniões dos sócios serão lavradas.

CAPÍTULO VI
Conselho Fiscal

ARTIGO 12 A sociedade não terá Conselho Fiscal.

CAPÍTULO VII

Anexo Contrato Social (0165188) SEI 19.09.02684.0011790/2021-22 / pg. 72

JUCESP
29 04 16

Exercício Social, Demonstrações Financeiras e Destinação do Lucro

ARTIGO 13 O exercício social encerra-se em 31 de dezembro de cada ano, quando serão elaboradas as Demonstrações Financeiras previstas em lei, as quais serão submetidas à apreciação dos sócios independentemente da realização de reunião dos sócios. O lucro então verificado terá a destinação determinada pelo(s) sócio(s) representando a maioria do capital social.

PARÁGRAFO ÚNICO - A sociedade poderá levantar balanços semestrais ou de períodos inferiores, para fins de apuração e destinação do resultado do período neles compreendido, podendo eventual lucro, por deliberação dos sócios, ser distribuído ou capitalizado.

CAPÍTULO VIII
Continuação da Sociedade

ARTIGO 14 A exclusão, retirada, morte, incapacidade ou insolvência do sócio minoritário não acarretará a dissolução da sociedade.

PARÁGRAFO ÚNICO – No caso de exclusão, retirada, morte, declaração de incapacidade ou insolvência do sócio minoritário, as quotas de sua titularidade serão adquiridas pelo sócio majoritário pelo valor contábil das quotas, apurado com base em balanço especialmente levantado para tal fim. Tais quotas serão pagas em até 12 (doze) parcelas mensais, iguais e consecutivas, vencendo-se a primeira no prazo de 30 (trinta) dias contados da data do levantamento do referido balanço patrimonial. Nessa hipótese, o sócio majoritário deverá recompor o quadro social com terceiros em até 180 (cento e oitenta) dias.

PARÁGRAFO 2º – No caso de dissolução, recuperação judicial ou pedido ou declaração de falência do sócio majoritário, a sociedade continuará com o(s) sócio(s) remanescente(s) e com o liquidante, administrador ou representante legal do referido sócio.

CAPÍTULO IX
Liquidação

ARTIGO 15 No caso de liquidação da sociedade, o procedimento estabelecido em lei será adotado e observado, com a nomeação, por sócio(s) representando a maioria do capital social, de um ou mais liquidantes para operar a sociedade durante a liquidação.

CAPÍTULO X
Alterações

ARTIGO 16 Este Contrato Social poderá ser alterado, em qualquer de seus artigos e a qualquer tempo, mediante deliberação de sócio(s) representando, no

Anexo Contrato Social (0165188) SEI 19.09.02684.0011790/2021-22 / pg. 73

JUCESP
29 04 16

mínimo, 75% (setenta e cinco por cento) do capital social. A aprovação de sócio(s) representando, no mínimo, 75% (setenta e cinco por cento) do capital social também será necessária para a deliberação sobre a incorporação, a fusão e a dissolução da sociedade, ou a cessação do seu estado de liquidação."

Os sócios e a administradora **MARIA DAS GRAÇAS VUOLO SAJOVIC STEFANINI**, acima qualificados, declaram, sob as penas da lei, que não estão impedidos de exercer a administração da sociedade, por lei especial, ou em virtude de condenação criminal, ou por se encontrarem sob os efeitos dela, a pena que vede, ainda que temporariamente, o acesso a cargos públicos; ou por crime falimentar, de prevaricação, peita ou suborno, concussão, peculato, ou contra a economia popular, contra o sistema financeiro nacional, contra normas de defesa da concorrência, contra as relações de consumo, fé pública, ou a propriedade.

ARTIGO 17 Fica designada a Sra. Maria das Graças Vuolo Sajovic Stefanini, responsável pela sociedade perante o CNPJ, em observância ao disposto na Instrução Normativa 1.183, de 19/08/2011, da Receita Federal do Brasil.

E, POR ESTAREM ASSIM JUSTAS E CONTRATADAS, as partes assinam o presente instrumento em 03 (três) vias de igual teor e forma, na presença de duas testemunhas.

Jaguariúna, 04 de abril de 2016.

Cartório Registro Civil 39º

STEFANINI PARTICIPAÇÕES LTDA.
p. Maria das Graças V. Sajovic Stefanini – Diretora

Cartório Registro Civil 39º

MARCO ANTÔNIO SILVA STEFANINI

Diretor:

Cartório Registro Civil 39º

MARCO ANTÔNIO SILVA STEFANINI

Visto do Advogado:

Cartório Registro Civil 39º

Bruna Marcucci Pedro
OAB/SP nº 337.533

TESTEMUNHAS:

1. _____
Nome:
RG nº: [redacted]

2. _____
Nome:
RG nº: [redacted]

Anexo Contrato Social (0165188) SEI 19.09.02684.0011790/2021-22 / pg. 74


39° Cartório
Registro Civil das Pessoas Naturais
Av. Brig. Faria Lima, 382 - CEP: 05426-200 - Fone: (11) 3816-7700
Andréa Ruzzante Gagliardi - OFICIAL TITULAR
Selo(s): 2 Atos 1072AA – 489342 1072AA – 489343
Reconheço por semelhança a firma de: (1) MARIA DAS GRAÇAS VUOLO SAJOVIC
STEFANINI. (2) MARCO ANTONIO SILVA STEFANINI e (1) BRUNA MARCUCCI PED
um documento com valor econômico, dou fé.
SÃO PAULO, 05 de abril de 2016
Em testemunho da verdade.
ANDRÉA MARIA DOS REIS – ESCREVENTE AUTORIZADO
(VALOR UNIT.R$ 8,15;QTD:(4) TOTAL R$ 32,60)
39º SUBD. VILA MADALENA
Andréa Maria dos Reis
Escrevente Autorizada
1072AA489342
1072AA489343

SECRETARIA DE DESENVOLVIMENTO
ECONÔMICO, CIÊNCIA,
TECNOLOGIA E INOVAÇÃO
JUCESP
NIRE
FLÁVIA R. BRITTO GONÇALVES
SECRETÁRIA GERAL
CERTIFICO O REGISTRO
SOB O NÚMERO
3522984425-1
JUCESP
JUNTA COMERCIAL DO ESTADO DE SÃO PAULO
29 ABR 2016

JUCESP 24 06 16

JUCESP PROTOCOLO
0.607.488/16-5

INSTRUMENTO PARTICULAR DE 1ª ALTERAÇÃO AO CONTRATO SOCIAL E ASSEMBLEIA GERAL DE TRANSFORMAÇÃO DA "STF PROJETOS E SERVIÇOS DE TECNOLOGIA DE DEFESA LTDA." EM SOCIEDADE ANÔNIMA

CNPJ/MF Nº 24.691.488/0001-09
NIRE 35.229.844.251

Pelo presente instrumento particular, as partes abaixo:

1. **MARCO ANTÔNIO SILVA STEFANINI**, [redacted]

2. **STEFANINI PARTICIPAÇÕES S.A.**, sociedade anônima com sede na cidade de Barueri, Estado de São Paulo, na Calçada das Margaridas, 163, sala 2, Centro Comercial de Alphaville, CEP 06453-038, inscrita no CNPJ/MF sob o nº 04.300.049/0001-10, com seus atos constitutivos devidamente registrados perante a Junta Comercial do Estado de São Paulo sob o NIRE 3530049067-3, neste ato representada na forma de seu estatuto social por seu Diretor, Sr. **Marco Antônio Silva Stefanini**, acima qualificado,

sócios detentores da totalidade do capital social da **STF PROJETOS E SERVIÇOS DE TECNOLOGIA DE DEFESA LTDA.**, com sede na cidade de Jaguariúna, Estado de São Paulo, na Avenida Marginal, n. 156, Sala 03, Centro, CEP 13820-000, inscrita no CNPJ/MF sob o nº 24.691.488/0001-09, com seus atos constitutivos devidamente registrados perante a Junta Comercial do Estado de São Paulo sob o NIRE 35.229.844.251, em sessão de 29 de abril de 2016 ("Sociedade"),

têm entre si, justo e acordado, alterar o tipo societário da Sociedade, mediante os seguintes termos e condições:

1. TRANSFORMAÇÃO DO TIPO SOCIETÁRIO DA SOCIEDADE

1.1. Nesta data, os sócios **MARCO ANTÔNIO SILVA STEFANINI** e **STEFANINI PARTICIPAÇÕES S.A.**, acima qualificados, resolvem, de comum acordo, nos termos dos Artigos 1.113 e seguintes da Lei 10.406/02, conforme alterada ("Código Civil"), aprovar a transformação do tipo jurídico da Sociedade, de sociedade empresária limitada para sociedade anônima, sem direito de recesso, de forma que a Sociedade passará a operar sob a denominação de "**STF PROJETOS E SERVIÇOS DE TECNOLOGIA DE DEFESA S.A.**" ("Companhia"), sendo certo que a transformação de tipo societário ora aprovada não importará em solução de continuidade da Companhia, a qual continuará existindo com os mesmos direitos e obrigações sociais, conservando o mesmo patrimônio social, a mesma escrituração comercial e fiscal.

Anexo Contrato Social (0165188) SEI 19.09.02684.0011790/2021-22 / pg. 76

JUCESP
24 06 16

1.2. Em virtude da transformação aprovada na forma do item 1.1. acima, a Companhia passa a ser regida pelas disposições da Lei 6.404/76, conforme alterada ("Lei das Sociedades por Ações") e as quotas de emissão da Companhia, totalmente subscritas e integralizadas, são neste ato convertidas em ações ordinárias, nominativas e sem valor nominal, na proporção de 1 (uma) ação ordinária, para cada quota de emissão da Companhia, mantendo-se a atual participação dos sócios, na forma dos Boletins de Subscrição contidos na ata de Assembleia Geral Extraordinária de Transformação na forma do Anexo I, nos termos do quadro abaixo:

ACIONISTAS	*AÇÕES ORDINÁRIAS*
STEFANINI PARTICIPAÇÕES S.A.	999
MARCO ANTONIO SILVA STEFANINI	1
TOTAL	**1.000**

2. APROVAÇÃO DO ESTATUTO SOCIAL

2.1. Em decorrência dessa alteração, os agora acionistas resolveram reunir-se em Assembleia Geral Extraordinária de Transformação, nesta data, que aprova, dentre outras matérias, a transformação e o novo estatuto social da Companhia, cujos documentos vão anexos à presente alteração do contrato social, como Anexo I, todos os quais serão levados a registro na Junta Comercial do Estado de São Paulo, na forma da lei.

3. ELEIÇÃO DE ADMINISTRADORES

3.1. Os sócios resolvem eleger, para compor a Diretoria da Companhia, (i) o Sr. **Marco Antônio Silva Stefanini**, [redacted] na condição de Diretor Presidente; e (ii) a Sra. **Maria das Graças Vuolo Sajovic Stefanini**, [redacted] ocupar o cargo de Diretora, ambos para um mandato de três anos, a se encerrar na data da Assembleia Geral Ordinária que vier a aprovar as contas do exercício findo em 31 de dezembro de 2018. Os Diretores eleitos (i) declararam, sob as penas da lei, terem conhecimento das disposições do artigo 147 da Lei das Sociedades por Ações, preencherem os requisitos legais para integrarem a administração da Companhia e não estarem impedidos de exercer cargos administrativos por lei especial; em virtude de condenação criminal, ou por se encontrarem sob efeitos dela; em virtude de pena que vede, ainda que temporariamente, o acesso a cargos públicos; ou em decorrência do cometimento de crime falimentar, de prevaricação, peita ou suborno, concussão, peculato, ou contra a economia popular, contra o sistema financeiro nacional, contra normas de defesa da concorrência, contra as relações de consumo, fé pública, ou a propriedade; e (ii) são investidos em seus cargos mediante assinatura dos respectivos

JUCESP
24 06 16

Termos de Posse, conforme assinatura e arquivo em seu livro próprio, na sede da Companhia.

E, por estarem assim, justas e contratadas, as Partes assinam o presente Instrumento Particular de 1ª Alteração ao Contrato Social e Assembleia Geral de Transformação da "STF Projetos e Serviços de Tecnologia de Defesa Ltda." em Sociedade Anônima em 3 (três) vias de igual teor e forma, na presença das testemunhas abaixo.

Jaguariúna, 10 de maio de 2016.

Sócios:

STEFANINI PARTICIPAÇÕES S.A.

Marco Antonio Stefanini

MARCO ANTÔNIO SILVA STEFANINI

JUCESP
24 JUN 2016

SECRETARIA DE DESENVOLVIMENTO ECONÔMICO, CIÊNCIA, TECNOLOGIA E INOVAÇÃO
JUCESP
CERTIFICO O REGISTRO SOB O NÚMERO
FLÁVIA REGINA BRITTO
SECRETÁRIA GERAL
272.875/16-8

JUCESP

Diretores eleitos:

Marco Antonio Stefanini

MARCO ANTÔNIO SILVA STEFANINI
Diretor Presidente

MARIA DAS GRAÇAS VUOLO SAJOVIC STEFANINI
Diretora

JUCESP
24 JUN 2016

SEDE
SECRETARIA DE DESENVOLVIMENTO ECONÔMICO, CIÊNCIA, TECNOLOGIA E INOVAÇÃO
JUCESP
CERTIFICO O REGISTRO SOB O NÚMERO
FLÁVIA REGINA BRITTO
SECRETÁRIA GERAL EM EXERCÍCIO
3530049265-0

JUCESP

Advogado:

Roberto Lourenço Belluzzo
OAB/SP 147.215

Testemunhas:

1.
Nome: Meire Lauri
RG nº: Gestora Financeira
CPF: [redacted]
RG

2.
Nome: Esdras Vieira Nascimento
RG nº: RG: [redacted]

JUCESP
24 06 16

Anexo I

STF PROJETOS E SERVIÇOS DE TECNOLOGIA DE DEFESA LTDA.
CNPJ/MF No. 24.691.488/0001-09
NIRE No.

ATA DA ASSEMBLEIA GERAL EXTRAORDINÁRIA REALIZADA EM 10 DE MAIO DE 2016, PARA TRANSFORMAÇÃO DA SOCIEDADE EMPRESÁRIA LIMITADA EM SOCIEDADE ANÔNIMA, COM A ADOÇÃO DA DENOMINAÇÃO SOCIAL DE "STF PROJETOS E SERVIÇOS DE TECNOLOGIA DE DEFESA S.A."

1. **Data, Hora e Local**: No dia 10 de maio de 2016, às 9:00 horas, na sede social da STF Projetos e Serviços de Tecnologia de Defesa Ltda., na Avenida Marginal, n. 156, Sala 03, Centro, na cidade de Jaguariúna, Estado de São Paulo, CEP 13820-000.

2. **Presença e Convocação**: Convocação dispensada, nos termos do artigo 1.072, §2º, da Lei nº. 10.406/02, conforme alterada ("Código Civil") e artigo 124, §4º da Lei 6.404, de 15 de dezembro de 1976, conforme alterada ("Lei das Sociedades por Ações"), em virtude da presença de sócios representando a totalidade do capital da sociedade, conforme consta do livro de presença.

3. **Mesa**: Presidente: Marco Antônio Silva Stefanini; Secretário: Roberto Lourenço Belluzzo.

4. **Ordem do dia**: (i) a transformação do tipo jurídico da sociedade, de sociedade empresária limitada para sociedade anônima de capital fechado; (ii) análise e aprovação do Estatuto Social; (iii) eleição de membros da Diretoria, fixando-lhes a remuneração global anual; (iv) instalação do Conselho Fiscal; e (v) demais assuntos de interesse da sociedade.

5. **Deliberações**: Por unanimidade de votos dos presentes, foram tomadas as seguintes deliberações, sem quaisquer reservas e/ou ressalvas:

   a) **aprovar** a transformação do tipo jurídico da sociedade empresária limitada para sociedade anônima de capital fechado, na forma dos artigos 1.113 e seguintes do Código Civil e artigos 220 e seguintes da Lei das Sociedades por Ações, que passará a operar sob a denominação de "**STF Projetos e Serviços de Tecnologia de Defesa S.A.**" ("Companhia"), sendo certo que a transformação de tipo societário ora aprovada não importará em solução de continuidade da Companhia, a qual continuará existindo com os mesmos direitos e obrigações sociais, conservando o mesmo patrimônio social, a mesma escrituração comercial e fiscal, renunciando expressamente os acionistas presentes ao direito de retirada;

   b) em virtude da transformação do tipo jurídico aprovada na forma do item (a) acima, a Companhia passa a ser regida pelas disposições legais da Lei das Sociedades por Ações e a totalidade das quotas de

Anexo Contrato Social (0165188) SEI 19.09.02684.0011790/2021-22 / pg. 79

JUCESP
24 08 16

emissão da Companhia, totalmente subscritas e integralizadas, são convertidas em ações ordinárias nominativas e sem valor nominal, à razão de 1:1, mantendo-se a atual participação dos sócios, nos termos do quadro abaixo, conforme boletins de subscrição assinados nesta data, que rubricados pelo Presidente e Secretário da Mesa, são anexados à presente Ata como Anexo A:

ACIONISTAS	AÇÕES ON	%
STEFANINI PARTICIPAÇÕES S.A.	999	99,9%
MARCO ANTÔNIO SILVA STEFANINI	1	0,1%
TOTAL	**1.000**	**100,0%**

c) **aprovar** o projeto do Estatuto Social Companhia, nos termos do Anexo B à presente ata, que, rubricado pelo Presidente e Secretário da Mesa, será levado a arquivamento na Junta Comercial juntamente com a presente ata, declarando efetiva e formalmente concretizada a transformação da sociedade em uma sociedade anônima;

d) **aprovar** a eleição, para compor a Diretoria da Companhia, (i) do Sr. **Marco Antônio Silva Stefanini,** [redacted] (ii) da Sra. **Maria das Graças Vuolo Sajovic Stefanini**, brasileira, [redacted] para ocupar o cargo de Diretora, ambos para um mandato de três anos, a se encerrar na data da Assembleia Geral Ordinária que vier a aprovar as contas do exercício findo em 31 de dezembro de 2018, sendo investidos nos seus respectivos cargos nesta data mediante assinatura dos respectivos Termos de Posse, lavrados em livro próprio. Os Diretores ora eleitos declaram, sob as penas da Lei, que não estão incursos em quaisquer crimes previstos em Lei ou restrições legais, que possam impedi-los de exercerem atividades empresariais e que não estão impedidos de exercerem a administração da Companhia, por lei especial, ou em virtude de condenação criminal ou por se encontrar sob os efeitos dela, a pena que vede, ainda que temporariamente, o acesso a cargos públicos; ou por crime falimentar, de prevaricação, peita ou suborno, concussão, peculato; ou contra a economia popular, contra o sistema financeiro nacional, contra as normas de defesa da concorrência, contra as relações de consumo, fé pública, ou a propriedade;

e) **fixar** a remuneração anual da Diretoria em R$1.000,00 (um mil reais);

f) **não instalar** o Conselho Fiscal; e

Anexo Contrato Social (0165188) SEI 19.09.02684.0011790/2021-22 / pg. 80

JUCESP
24 06 16

g) **autorizar** a Diretoria da Companhia proceder à atualização dos registros e anotações junto aos órgãos públicos competentes para que conste a transformação da Companhia em sociedade anônima, informando sua nova denominação social, bem como aprovar a lavratura e publicação da presente Ata sob a forma de extrato ou sumário dos fatos ocorridos, nos termos dos §§ 1º e 3º do Artigo 130 da LSA.

6. **Encerramento**: Nada mais havendo a tratar, o Sr. Presidente ofereceu a palavra a quem dela quisesse fazer uso e, como ninguém a pedisse, declarou encerrados os trabalhos e suspensa a assembleia pelo tempo necessário à lavratura desta ata, a qual, reaberta a sessão, foi lida, aprovada e por todos os presentes assinada e rubricada, juntamente com os Anexos A e B que ficam arquivados na sede social.

Jaguariúna, 10 de maio de 2016.

Mesa:

Marco Antônio Silva Stefanini
(Presidente)

Roberto Lourenço Belluzzo
(Secretário)

Acionistas:

Stefanini Participações S.A.
p. Marco Antônio Silva Stefanini

Marco Antônio Silva Stefanini

Advogado:

Roberto Lourenço Belluzzo
OAB/SP 147.215

Anexo Contrato Social (0165188) SEI 19.09.02684.0011790/2021-22 / pg. 81

Anexo Contrato Social (0165188) SEI 19.09.02684.0011790/2021-22 / pg. 82

Anexo A - Autenticação da Mesa da Assembleia Geral Extraordinária de Transformação, realizada em 10 de maio de 2016.

Marco Antonio Stefanini
Presidente da Mesa

Secretário da Mesa

BOLETIM DE SUBSCRIÇÃO DO CAPITAL SOCIAL DA STF PROJETOS E SERVIÇOS DE TECNOLOGIA DE DEFESA S.A.
CNPJ/MF No. 24.691.488/0001-09
NIRE No.

Capital: R$1.000,00 (um mil reais), dividido em 1.000 (uma mil) ações ordinárias nominativas, sem valor nominal
Preço de Emissão: R$ 1,00 por ação

Nº de Ordem	Subscritor	Nacionalidade	Residência/Sede	Nº de Ações Ordinárias Subscritas	Valor pago pelas Ações	Forma de Integralização
01	**STEFANINI PARTICIPAÇÕES S.A.**, sociedade por ações, inscrita no CNPJ sob nº 04.300.049/0001-10 com seus atos constitutivos devidamente registrados perante a Junta Comercial do Estado de São Paulo sob o NIRE 3530049067-3, por seu Diretor Marco Antonio Stefanini (assinatura)	Brasileira	Calçada das Margaridas, nº 163, Sala 2, Centro Comercial Alphaville, na cidade de Barueri, Estado de São Paulo, CEP 06453-000	999	999,00	Conversão de quotas anteriormente subscritas no capital social da STF PROJETOS E SERVIÇOS DE TECNOLOGIA DE DEFESA LTDA.
02	**MARCO ANTÔNIO SILVA STEFANINI**, brasileiro, casado sob o regime de comunhão universal de bens, empresário e geólogo, portador da Cédula de Identidade RG nº. 10.153.181-3 SSP/SP, e do CPF nº. 042.501.968-36 Marco Antonio Stefanini (assinatura)	Brasileira	Praça dos Carvalhos, L14, condomínio duas Marias, na cidade de Jaguariúna, Estado de São Paulo, CEP 13820-000.	1	1,00	Conversão de quotas anteriormente subscritas no capital social da STF PROJETOS E SERVIÇOS DE TECNOLOGIA DE DEFESA LTDA.
			TOTAL	1.000	**R$1.000,00**	

JUCESP
24 06 16

Anexo B - Autenticação da Mesa da Assembleia Geral Extraordinária de Transformação, realizada em 10 de maio de 2016.

Marco Antonio Stefanini
Presidente da Mesa

Secretário da Mesa

"ESTATUTO SOCIAL DA STF PROJETOS E SERVIÇOS DE TECNOLOGIA DE DEFESA S.A.

CAPÍTULO I - Da Denominação, Sede, Prazo de Duração e Objeto Social

Artigo 1º - A "**STF PROJETOS E SERVIÇOS DE TECNOLOGIA DE DEFESA S.A.**" é uma sociedade anônima de capital fechado regida pelo presente estatuto e pelas disposições legais que lhe forem aplicáveis.

Artigo 2º - A companhia tem sede na Avenida Marginal, n. 156, Sala 03, Centro, na Cidade de Jaguariúna, Estado de São Paulo, CEP 13820-000, podendo, a critério da Diretoria, abrir filiais, agências, escritórios ou sucursais em qualquer parte do país ou no exterior.

Artigo 3º - A companhia tem prazo de duração indeterminado.

Artigo 4º - A companhia tem por objeto (i) a prestação de serviços de tecnologia industrial básica, projetos, pesquisa, desenvolvimento e inovação tecnológicos, assistência técnica, consultoria e transferência de tecnologia de defesa, incluindo serviços técnicos especializados de defesa cibernética; (ii) o desenvolvimento de soluções de automação industrial, suporte técnico de informática e sistemas de defesa e de inteligência, incluindo atividades de comando e controle cibernéticos; (iii) o licenciamento e desenvolvimento de software próprio ou de terceiros de defesa; e (iv) a participação em outras sociedades de qualquer tipo societário, como sócia ou acionista.

CAPÍTULO II - Do Capital e das Ações

Artigo 5º - O capital social, totalmente subscrito e integralizado em moeda corrente nacional, é de R$ 1.000,00 (um mil reais), dividido em 1.000 (uma mil) ações ordinárias nominativas, sem valor nominal.

Artigo 6º - A cada ação ordinária corresponde um voto nas deliberações das Assembleias Gerais.

Artigo 7º - A ação é indivisível em relação à companhia. Quando a ação pertencer a mais de uma pessoa, os direitos a ela conferidos serão exercidos pelo representante do condomínio.

Artigo 8º - As ações não serão representadas por cautelas, presumindo-se a respectiva propriedade pela inscrição do nome do acionista no Livro de Registro de Ações Nominativas.

Artigo 9º - Nos casos de reembolso de ações, previstos em lei, o valor de reembolso corresponderá ao valor do patrimônio líquido das ações, de acordo com o último balanço aprovado pela Assembleia Geral, segundo os critérios de avaliação do ativo e

Anexo Contrato Social (0165188) SEI 19.09.02684.0011790/2021-22 / pg. 83

JUCESP
24 06 16

do passivo fixados na Lei das Sociedades por Ações e com os princípios contábeis geralmente aceitos.

CAPÍTULO III - Das Assembleias Gerais

Artigo 10 - As Assembleias Gerais serão convocadas por qualquer Diretor ou pelos acionistas, nos casos previstos em lei.

Parágrafo 1° - As Assembleias Gerais serão presididas pelo acionista escolhido por maioria de votos dos presentes e secretariadas por quem o presidente da Assembleia indicar.

Parágrafo 2° - Só poderão tomar parte e votar na Assembleia Geral os acionistas cujas ações estejam inscritas em seu nome, no registro competente, até 3 (três) dias antes da data marcada para a sua realização.

Parágrafo 3° - As Assembleias Gerais da companhia serão ordinárias ou extraordinárias, realizando-se, ordinariamente, nos quatro primeiros meses seguintes ao encerramento do exercício social, de acordo com o artigo 132, Lei nº 6.404/76; e extraordinariamente, sempre que necessário.

Parágrafo 4° - As deliberações da Assembleia Geral, ressalvadas as hipóteses especiais previstas em lei, serão tomadas por maioria de votos dos presentes, não se computando os votos em branco, com exceção das decisões sobre as matérias relacionadas nos Artigos 11 e 12 deste instrumento.

Artigo 11 - As decisões sobre as seguintes matérias dependerão da aprovação de acionistas representando 75% (setenta e cinco por cento) do capital votante da companhia ou poderão exigir o voto favorável de determinados acionistas, caso assim determinado em Acordo de Acionistas:

(i) registro da companhia como companhia aberta;

(ii) quaisquer alterações do Estatuto Social, inclusive com relação às preferências, vantagens ou características das ações existentes, criação e novas classes de ações, bem como a realização de qualquer mudança no escopo das atividades sociais;

(iii) a cisão, fusão, incorporação envolvendo a companhia, sua transformação ou qualquer outra forma de reorganização societária;

(iv) a autorização aos administradores da companhia para confessar falência ou pedir concordata;

(v) a liquidação e dissolução da Companhia;

(vi) aprovação das contas da Diretoria e distribuição de resultados, a qualquer título, incluindo dividendos, respeitado o disposto no presente e/ou em Acordo de Acionistas;

(vii) aumento ou redução do capital social, desdobramento ou grupamento de ações, resgate, amortização ou compra de ações da própria companhia para cancelamento ou manutenção em tesouraria; criação e emissão, pública ou privada, resgate ou negociação de quaisquer títulos ou valores mobiliários da companhia, conversíveis ou não em ações, tais como ações preferenciais,

Anexo Contrato Social (0165188) SEI 19.09.02684.0011790/2021-22 / pg. 84

JUCESP
24 06 16

debêntures, bônus de subscrição, partes beneficiárias, ou opções de compra ou subscrição de ações; e

(viii) fixação da remuneração anual e global dos administradores.

Artigo 12 - As demais decisões dependerão da aprovação de acionistas representando 51% (cinquenta e um por cento) do capital votante da companhia.

CAPÍTULO IV - Da Administração

Artigo 13 - A companhia será administrada por uma Diretoria constituída por 2 (dois) Diretores, acionistas ou não, residentes no país, eleitos pela Assembleia Geral, que também fixará seus honorários.

Artigo 14 - O prazo de mandato da Diretoria é de 3 (três) anos, permitida a reeleição, mas qualquer que seja a data de eleição, os mandatos dos Diretores terminarão na data da Assembleia Geral que examinar as contas do último exercício social de suas gestões; outrossim, mesmo quando vencidos os respectivos mandatos, os Diretores continuarão no exercício de seus cargos até a eleição e posse dos novos Diretores.

Artigo 15 - A investidura no cargo de Diretor far-se-á por termo lavrado e assinado no livro de Atas de Reuniões da Diretoria, independentemente de caução.

Artigo 16 - Nos casos de impedimento, ausências temporárias ou vacância definitiva de um Diretor, compete aos Diretores remanescentes convocar Assembleia Geral para eleição de um substituto.

Artigo 17 - A Diretoria reunir-se-á sempre que convocada por qualquer de seus membros, com 3 (três) dias de antecedência.

Parágrafo 1º É dispensado o interregno de 3 (três) dias quando a Diretoria se reunir com a presença, ou representação, de todos os seus membros em exercício.

Parágrafo 2º Em todas as reuniões da Diretoria, é admitido que o Diretor ausente seja representado por um de seus pares, seja para formação de "*quorum*", seja para votação; e, igualmente, são admitidos votos por carta, telegrama, telex ou telefax, quando recebidos na sede social até o momento da reunião.

Parágrafo 3º Nas reuniões da Diretoria, as deliberações serão tomadas por maioria de votos, e constarão de atas lavradas e assinadas no livro próprio.

Artigo 18 - Além dos que forem necessários à realização dos fins sociais, a Diretoria fica investida de poderes para transigir, renunciar, desistir, firmar compromissos, confessar dívidas e fazer acordos, adquirir, alienar e onerar bens móveis e imóveis, nas condições deste estatuto.

Artigo 19 - Compete especialmente à Diretoria:

a) apresentar à Assembleia Geral o Relatório da Diretoria e as demonstrações financeiras previstas em lei, depois de submetidas ao parecer do conselho fiscal, se em operação;

Anexo Contrato Social (0165188) SEI 19.09.02684.0011790/2021-22 / pg. 85

JUCESP
24 06 16

b) deliberar sobre a instalação, transferência ou extinção de filiais, escritórios e outras dependências da companhia;

c) fixar a orientação geral dos negócios sociais, e fixar a política comercial e financeira da companhia;

d) propor à Assembleia Geral a destinação dos lucros do exercício, observadas as disposições legais e as deste estatuto.

Parágrafo Único Os Diretores dividirão entre si as atribuições da Diretoria, observado o disposto neste estatuto.

Artigo 20 - A companhia considerar-se-á obrigada quando representada:

a) isoladamente, nos atos normais de gestão que constituem atribuição da Diretoria;

b) conjuntamente, por dois procuradores, de acordo com os poderes que lhes houverem sido conferidos nos respectivos instrumentos de mandato;

c) isoladamente, por um procurador, de acordo com os poderes que lhes houverem sido conferidos no respectivo instrumento de mandato;

Artigo 21 - É permitido somente aos Diretores concederem fianças ou avais em nome da companhia, bem como contrair obrigações de qualquer natureza. Qualquer outra pessoa, mesmo que envolvida nesta companhia, não poderá conceder fianças ou avais em nome desta, bem como contrair obrigações de qualquer natureza, e se o fizer, responderá pessoalmente pela infringência desta cláusula.

CAPÍTULO V - Do Conselho Fiscal

Artigo 22 - A companhia não terá Conselho Fiscal permanente, sendo que este somente se instalará a pedido de acionistas que representem, no mínimo, 10% (dez por cento) das ações com direito a voto.

Artigo 23 - Caso solicitado seu funcionamento, os acionistas deverão determinar o número de membros efetivos e igual número de suplentes para compor o Conselho Fiscal; cada período de funcionamento do Conselho Fiscal terminará na primeira Assembleia Geral Ordinária após sua instalação.

Artigo 24 - A remuneração dos Conselheiros Fiscais será determinada pela Assembleia Geral que os eleger.

CAPÍTULO VI - Do Exercício Social e Distribuição de Lucros

Artigo 25 - O exercício social terminará no dia 31 de dezembro de cada ano, quando serão elaboradas as demonstrações financeiras previstas na legislação comercial e fiscal.

Artigo 26 - Dos lucros líquidos assim apurados, serão destinados:

a) 5% (cinco por cento), para o Fundo de Reserva Legal, até atingir 20% (vinte por cento) do capital social;

Anexo Contrato Social (0165188) SEI 19.09.02684.0011790/2021-22 / pg. 86

JUCESP
24 06 16

b) 25% (vinte e cinco por cento), para distribuição aos acionistas a título de dividendo obrigatório.

Parágrafo 1º O dividendo previsto neste artigo não será obrigatório no exercício social em que a Diretoria informar à Assembleia Geral Ordinária não ser ele compatível com a situação financeira da companhia. O Conselho Fiscal, se em funcionamento deverá dar parecer sobre essa informação. Os lucros que assim deixarem de ser distribuídos serão registrados como reserva especial e, se não absorvidos por prejuízos em exercícios subsequentes, deverão ser pagos como dividendos assim que o permitir a situação financeira da companhia.

Parágrafo 2º O saldo dos lucros líquidos terá a destinação que a Assembleia Geral determinar, podendo ser transferido para Reserva de Aumento de Capital ou outra reserva de lucros, cujos saldos, somados, não poderão ultrapassar o capital social; atingindo esse limite, a Assembleia Geral deliberará sobre a aplicação do excesso em aumento do capital social ou na distribuição de dividendos.

Parágrafo 3º A Assembleia Geral Ordinária poderá, desde que não haja oposição de qualquer acionista presente, deliberar a distribuição de dividendo inferior ao previsto neste artigo ou a retenção de todo o lucro.

Artigo 27 - A Diretoria poderá levantar balaços intermediários e declarar dividendos à conta de lucros apurados nesses balanços, observadas as restrições legais.

Artigo 28 - A Diretoria poderá declarar dividendos intermediários à conta de lucros acumulados ou de reservas de lucros existentes no último balanço anual ou semestral aprovado em assembleia.

CAPÍTULO VII - Da Liquidação

Artigo 29 - A companhia entrará em liquidação nos casos legais, cabendo à Assembleia Geral determinar o modo de liquidação e nomear o liquidante que deverá atuar nesse período.

CAPÍTULO VIII - Das disposições Finais

Artigo 30 - A qualquer tempo a companhia poderá transformar-se em outra forma jurídica, por decisão majoritária da Assembleia Geral.

Artigo 31 - Fica eleito o foro da Capital do Estado de São Paulo, para dirimir dúvidas e controvérsias oriundas deste estatuto.

Artigo 32 - Aos casos omissos aplicar-se-ão as disposições da Lei 6.404, de 15 de dezembro de 1976, conforme alterada".

Advogado:

Roberto Lourenço Belluzzo
OAB/SP 147.215

Anexo Contrato Social (0165188) SEI 19.09.02684.0011790/2021-22 / pg. 87

JUCESP
24 DR. 16

TERMO DE POSSE.

Nesta data, eu, **Maria das Graças Vuolo Sajovic Stefanini,** [redacted] tomo posse do cargo de Diretora da **STF PROJETOS E SERVIÇOS DE TECNOLOGIA DE DEFESA S.A.** ("Companhia"), conforme eleição aprovada no Instrumento Particular de 1ª Alteração do Contrato Social e Assembleia Geral Extraordinária de Transformação da Companhia, datada de 10 de maio de 2016.

Declaro, para os devidos fins, que o endereço acima é o endereço no qual receberei as citações e intimações em processos administrativos e judiciais relativos a atos de minha gestão na Companhia.

Declaro, ainda, sob as penas da lei, que não estou impedida de exercer a administração da Companhia por lei especial ou em virtude de condenação criminal, ou por se encontrar sob os efeitos dela, a pena que vede, ainda que temporariamente, o acesso a cargos públicos; ou por crime falimentar, de prevaricação, peita ou suborno, concussão, peculato, ou contra a economia popular, contra o sistema financeiro nacional, contra normas de defesa da concorrência, contra as relações de consumo, fé pública, ou a propriedade.

Jaguariúna, 10 de maio de 2016.

Maria das Graças Vuolo Sajovic Stefanini
Diretora

JUCESP
24 OUT 16

TERMO DE POSSE.

Nesta data, eu, **Marco Antônio Silva Stefanini,** [redacted] como posse do cargo de Diretor Presidente da **STF PROJETOS E SERVIÇOS DE TECNOLOGIA DE DEFESA S.A.** ("Companhia"), conforme eleição aprovada no Instrumento Particular de 1ª Alteração do Contrato Social e Assembleia Geral Extraordinária de Transformação da Companhia, datada de 10 de maio de 2016.

Declaro, para os devidos fins, que o endereço acima é o endereço no qual receberei as citações e intimações em processos administrativos e judiciais relativos a atos de minha gestão na Companhia.

Declaro, ainda, sob as penas da lei, que não estou impedido de exercer a administração da Companhia por lei especial ou em virtude de condenação criminal, ou por se encontrar sob os efeitos dela, a pena que vede, ainda que temporariamente, o acesso a cargos públicos; ou por crime falimentar, de prevaricação, peita ou suborno, concussão, peculato, ou contra a economia popular, contra o sistema financeiro nacional, contra normas de defesa da concorrência, contra as relações de consumo, fé pública, ou a propriedade.

Jaguariúna, 10 de maio de 2016.

Marco Antonio Stefanini

Marco Antônio Silva Stefanini
Diretor Presidente

JUCESP
24 02 17

JUCESP PROTOCOLO
0.173.833/17-2

STF PROJETOS E SERVIÇOS DE TECNOLOGIA DE DEFESA S.A.
CNPJ/MF nº 24.691.488/0001-09
NIRE 35.300.492.650

ATA DA ASSEMBLEIA GERAL EXTRAORDINÁRIA REALIZADA EM 09 DE JANEIRO DE 2017

I. Data, Hora e Local: Realizada no dia 09 de janeiro de 2017, às 10h, na Avenida Eusébio Matoso, 1.375, 8º Andar, cidade e Estado de São Paulo, CEP 05423-905.

II. Convocação e Presença: Dispensada a publicação de editais de convocação, nos termos do disposto no Artigo 124, § 4º da Lei nº 6.404/76 ("Lei das S.A."), tendo em vista a presença da totalidade dos acionistas da Companhia, conforme assinaturas lançadas no "Livro de Presença de Acionistas".

III. Composição da Mesa: Sr. Marco Antônio Silva Stefanini (Presidente) e Sr. Roberto Lourenço Belluzzo (Secretário).

IV. Leitura de Documentos, Recebimento de Votos e Lavratura da Ata: (1) Dispensada a leitura dos documentos relacionados às matérias deliberadas na Assembleia, uma vez que o seu conteúdo é do inteiro conhecimento dos acionistas; (2) As declarações de voto, protestos e dissidências, porventura apresentadas, foram recebidas, numeradas e autenticadas pela Mesa e ficarão arquivadas na sede da Companhia, nos termos do artigo 130, §1º, da Lei das S.A.; e (3) Autorizada a lavratura da presente ata na forma de sumário, nos termos do artigo 130, §1º, da Lei das S.A.

V. Ordem do dia: (1) criação de nova espécie de ações e definição dos seus respectivos direitos e vantagens; (2) aumento do capital social; (3) reforma do estatuto social; (4) eleição dos membros do conselho de administração da Companhia; e (5) fixação da remuneração anual global dos membros da administração da Companhia.

VI. Deliberações: Após análise e discussões sobre as matérias constantes da ordem do dia, decidiu-se, por unanimidade e sem quaisquer restrições:

(1) aprovar a criação de uma nova espécie de ação da Companhia: ações preferenciais. As ações preferencias ora criadas serão nominativas e sem valor nominal e terão as seguintes características, direitos e vantagens: (a) não terão direito a voto nas deliberações das assembleias gerais, exceto nas hipóteses previstas em lei e nos casos estabelecidos pelos acionistas; (b) outorgarão aos seus titulares prioridade no reembolso do capital, sem prêmio, nos termos do artigo 17, parágrafo II, da Lei nº 6.404/76; (c) participarão, em igualdade de condições com as ações ordinárias, na distribuição de dividendos pela Companhia ou de qualquer outra forma de pagamento de remuneração aos acionistas; e (d) serão automaticamente conversíveis em ações ordinárias nominativas e sem valor nominal, à razão de 1:1, nos casos estabelecidos pelos acionistas.

(2) aprovar o aumento do capital social da Companhia em R$4.771.782,00 (quatro milhões, setecentos e setenta e um mil, setecentos e oitenta e dois reais), mediante a emissão de 2.385.391 (dois milhões, trezentas e oitenta e cinco mil, trezentas e noventa e uma) ações ordinárias e 2.386.391 (dois milhões, trezentas e oitenta e seis mil, trezentas e noventa e uma) ações preferenciais, todas nominativas e sem valor nominal, ao preço de emissão de R$1,00 (um real) por ação. Dessa forma, o capital social da Companhia, atualmente no valor de R$1.000,00

Anexo Contrato Social (0165188) SEI 19.09.02684.0011790/2021-22 / pg. 90

(um mil reais), dividido em 1.000 (uma mil) ações ordinárias nominativas e sem valor nominal, passa a ser de R$4.772.782,00 (quatro milhões, setecentos e setenta e dois mil, setecentos e oitenta e dois reais), dividido em 4.772.782 (quatro milhões, setecentas e setenta e duas mil, setecentas e oitenta e duas) ações, sendo 2.386.391 (dois milhões, trezentas e oitenta e seis mil, trezentas e noventa e uma) ações ordinárias e 2.386.391 (dois milhões, trezentas e oitenta e seis mil, trezentas e noventa e uma) ações preferenciais, todas nominativas e sem valor nominal.

Conforme consta nos Boletins de Subscrição, que são parte integrante da presente ata na forma dos Anexos I.A e I.B, a acionista STEFANINI PARTICIPAÇÕES S.A. subscreve 1.430.835 (um milhão, quatrocentas e trinta mil, oitocentas e trinta e cinco) ações ordinárias e 954.556 (novecentas e cinquenta e quatro mil, quinhentas e cinquenta e seis) ações preferenciais emitidas neste ato, e RAFAEL ADVANCED DEFENSE SYSTEMS LTD. subscreve as demais 954.556 (novecentas e cinquenta e quatro mil, quinhentas e cinquenta e seis) ações ordinárias e 1.431.835 (um milhão, quatrocentas e trinta e uma mil, oitocentas e trinta e cinco) ações preferenciais emitidas neste ato. A integralização das ações ora subscritas pelas partes acima dar-se-á conforme os Boletins de Subscrição anexos à presente.

O aumento do capital social da Companhia é implementado com o expresso consentimento da acionista STEFANINI PARTICIPAÇÕES S.A., que o aprovou em todos os seus termos e renunciou parcialmente em favor da RAFAEL ADVANCED DEFENSE SYSTEMS LTD. o seu direito de preferência na subscrição das novas ações.

(3) aprovar a proposta para reforma do Estatuto Social da Companhia, de modo a (i) refletir a criação das ações preferenciais sem direito a voto deliberada no item (1) acima; (ii) refletir o aumento do capital social deliberado no item (2) acima; (iii) alterar a denominação social da Companhia de "STF PROJETOS E SERVICOS DE TECNOLOGIA DE DEFESA S.A." para "STEFANINI RAFAEL SEGURANÇA E DEFESA S.A."; (iv) ajustar o texto do objeto social, (v) alterar as competências da assembleia geral; (vi) criar um conselho de administração e determinar sua composição, funcionamento e competências; (vii) alterar composição, funcionamento e competências da diretoria da Companhia; (viii) estabelecer arbitragem como o mecanismo para resolução de controvérsias; e (ix) refletir as demais práticas, políticas e estruturas de governança corporativa considerando a atual composição acionária da Companhia. Em consequência das deliberações ora adotadas, o Estatuto Social consolidado, contemplando todas as alterações aprovadas, assim como outros ajustes pontuais de redação, passa a vigorar na forma do Anexo II à presente ata.

(4) aprovar a eleição dos Srs. (i) **Marco Antônio Silva Stefanini**, cidadão brasileiro, casado, empresário e geólogo, portador da cédula de identidade RG nº 10.153.181-3 SSP/SP, e inscrito no CPF/MF sob o nº 042.501.968-36, residente e domiciliado na cidade de Jaguariúna, Estado de São Paulo, na Praça dos Carvalhos, L14, Condomínio Duas Marias, CEP: 13820-000; (ii) **Wander Marques Cunha**, cidadão brasileiro, casado, engenheiro da computação, portador da cédula de identidade nº 5060482083 – CREA/SP, inscrito no CPF/MF sob o nº 201.669.288-01, residente e domiciliado na cidade e Estado de São Paulo, na Rua da Meação, 197, apt. 22, Vila Regente Feijó, CEP: 03335-045, (iii) **Marcos Pereira de Almeida**, cidadão brasileiro, casado, administrador de empresas, portador da cédula de identidade RG nº 26.840.317-X - SSP/SP e inscrito no CPF/MF sob o nº 165.784.298-32, residente e domiciliado na cidade e Estado de São Paulo, na Rua Padre Carvalho, 295, Apartamento 171, CEP: 05427-100; (iv) **Avi Krengel**, cidadão israelense, casado, administrador, portador da cédula de identidade de estrangeiro - RNE nº V 945091-I, residente e domiciliado na cidade e Estado de São Paulo, na Rua João Lourenço, nº 713/151, CEP: 04508-031; e (v) **Ariel Karo**, cidadão israelense, casado, administrador, portador do passaporte nº 13574223, emitido pelo Estado de Israel, residente e domiciliado em 73 Herzel St. Kfar-Saba, Estado de Israel, para comporem o Conselho de Administração da Companhia, todos com um mandato de 3 (três) anos, que se encerrará na data da Assembleia Geral Ordinária da Companhia a ser realizada em 2019.

Os membros do Conselho de Administração ora eleitos declararam, nesta data, sob as penas da lei, que não estão impedidos, por lei especial, de exercer a administração de sociedades, nem condenados ou sob efeitos de condenação, a pena que vede, ainda que temporariamente, o acesso

Anexo Contrato Social (0165188) SEI 19.09.02684.0011790/2021-22 / pg. 91

a cargos públicos; ou por crime falimentar, de prevaricação, peita ou suborno, concussão, peculato; ou contra a economia popular, a fé pública ou a propriedade, bem como cumprem com os demais requisitos da Lei nº 6.404/76. Dessa forma, os membros do Conselho de Administração ora eleitos tomam posse em seus cargos, mediante a assinatura dos respectivos Termos de Posse no Livro de Atas de Reunião do Conselho de Administração.

(5) fixar o montante global da remuneração anual dos administradores da Companhia, nos termos da proposta apresentada pela administração e arquivada na sede da Companhia.

VII. Encerramento: Nada mais havendo a tratar e, como ninguém mais desejava fazer uso da palavra, foram encerrados os trabalhos e a presente ata foi lavrada, tendo sido lida, achada conforme e assinada pelos presentes.

São Paulo (SP), 09 de janeiro de 2017.

Marco Antônio Silva Stefanini
Presidente

Roberto Lourenço Belluzzo
Secretário

Acionistas:

STEFANINI PARTICIPAÇÕES S.A.
p. Marco Antônio Silva Stefanini

RAFAEL ADVANCED DEFENSE SYSTEMS LTD.
pp. Fabiano Gallo

JUCESP
24 FEV 2017
SEDE
SECRETARIA DE DESENVOLVIMENTO ECONÔMICO, CIÊNCIA, TECNOLOGIA E INOVAÇÃO
JUCESP
CERTIFICO O REGISTRO SOB O NÚMERO
106.436/17-0
FLÁVIA REGINA DE SOUZA OLIVEIRA
SECRETÁRIA GERAL
JUCESP

Anexo Contrato Social (0165188) SEI 19.09.02684.0011790/2021-22 / pg. 92

ANEXO I.A

(Ata da Assembleia Geral Extraordinária da STF Projetos e Serviços de Tecnologia de Defesa S.A., realizada em 09 de janeiro de 2017)

- BOLETIM DE SUBSCRIÇÃO -

EMISSOR: STF PROJETOS E SERVICOS DE TECNOLOGIA DE DEFESA S.A. (atualmente STEFANINI RAFAEL SEGURANÇA E DEFESA S.A.), companhia fechada, com sede na cidade e Estado de São Paulo, na Avenida Eusébio Matoso, 1.375, 8º Andar, salas 801 e 802, Butantã, CEP 05423-905, inscrita perante o Cadastro Nacional da Pessoa Jurídica do Ministério da Fazenda ("CNPJ/MF") sob o nº 24.691.488/0001-09 e registrada na Junta Comercial do Estado de São Paulo sob o NIRE 35.300.492.650 ("Companhia").

SUBSCRITOR: STEFANINI PARTICIPAÇÕES S.A., sociedade anônima, com sede na cidade de Barueri, Estado de São Paulo, na Calçada das Margaridas, nº 163, 1º andar, sala 2, Condomínio Centro Comercial de Alphaville, CEP 06453-038, inscrita perante o CNPJ/MF sob o nº. 4.300.049/0001-10 e registrada na Junta Comercial do Estado de São Paulo sob o NIRE 35.300.49067-3 ("Stefanini").

DELIBERAÇÃO: Assembleia Geral Extraordinária realizada no dia 09 de janeiro de 2017.

SUBSCRIÇÃO: Subscrição de 1.430.835 (um milhão, quatrocentas e trinta mil, oitocentas e trinta e cinco) ações ordinárias e 954.556 (novecentas e cinquenta e quatro mil, quinhentas e cinquenta e seis) ações preferenciais, todas nominativas e sem valor nominal ("Ações Subscritas").

PREÇO DE EMISSÃO: O preço de emissão de cada ação é de R$1,00 (um real).

VALOR TOTAL DA SUBSCRIÇÃO: O valor total da subscrição é de R$2.385.391,00 (dois milhões, trezentos e oitenta e cinco mil, trezentos e noventa e um reais).

FORMA DE INTEGRALIZAÇÃO: A integralização da totalidade das Ações Subscritas deverá ser realizada, em moeda corrente nacional, até o dia 23 de janeiro de 2017.

São Paulo (SP), 09 de janeiro de 2017.

Marco Antonio Stefanini

STEFANINI PARTICIPAÇÕES S.A.
p. Marco Antônio Silva Stefanini

Marco Antonio Stefanini
Marco Antônio Silva Stefanini
Presidente

Roberto Lourenço Belluzzo
Secretário

Anexo Contrato Social (0165188) SEI 19.09.02684.0011790/2021-22 / pg. 93

ANEXO I.B

(Ata da Assembleia Geral Extraordinária da STF Projetos e Serviços de Tecnologia de Defesa S.A., realizada em 09 de janeiro de 2017)

- BOLETIM DE SUBSCRIÇÃO -

EMISSOR: STF PROJETOS E SERVICOS DE TECNOLOGIA DE DEFESA S.A. (atualmente STEFANINI RAFAEL SEGURANÇA E DEFESA S.A.), companhia fechada, com sede na cidade de e Estado de São Paulo, na Avenida Eusébio Matoso, 1.375, 8º Andar, salas 801 e 802, Butantã, CEP 05423-905, inscrita perante o Cadastro Nacional da Pessoa Jurídica do Ministério da Fazenda ("CNPJ/MF") sob o nº 24.691.488/0001-09 e registrada na Junta Comercial do Estado de São Paulo sob o NIRE 35.300.492.650 ("Companhia").

SUBSCRITOR: RAFAEL ADVANCED DEFENSE SYSTEMS LTD., sociedade organizada e existente de acordo com as leis de Israel, com sede na P.O. Box 2250, Haifa 31021, Israel, inscrita no CNPJ/MF sob o número 13.476.335/0001-22 ("Rafael").

DELIBERAÇÃO: Assembleia Geral Extraordinária realizada no dia 09 de janeiro de 2017.

SUBSCRIÇÃO: Subscrição de 954.556 (novecentas e cinquenta e quatro mil, quinhentas e cinquenta e seis) ações ordinárias e 1.431.835 (um milhão, quatrocentas e trinta e uma mil, oitocentas e trinta e cinco) ações preferenciais, todas nominativas e sem valor nominal ("Ações Subscritas").

PREÇO DE EMISSÃO: O preço de emissão de cada ação é de R$1,00 (um real).

VALOR TOTAL DA SUBSCRIÇÃO: O valor total da subscrição é de R$2.386.391,00 (dois milhões, trezentos e oitenta e seis mil, trezentos e noventa e um reais).

FORMA DE INTEGRALIZAÇÃO: A integralização da totalidade das Ações Subscritas deverá ser realizada, em moeda corrente nacional, até o dia 23 de janeiro de 2017.

São Paulo (SP), 09 de janeiro de 2017.

RAFAEL ADVANCED DEFENSE SYSTEMS LTD.
p. Fabiano Gallo

Marco Antônio Silva Stefanini
Presidente

Roberto Lourenço Belluzzo
Secretário

Anexo Contrato Social (0165188) SEI 19.09.02684.0011790/2021-22 / pg. 94

JUCESP

ANEXO II

(Ata da Assembleia Geral Extraordinária da STF Projetos e Serviços de Tecnologia de Defesa S.A., realizada em 09 de janeiro de 2017)

- ESTATUTO SOCIAL -

Anexo Contrato Social (0165188) SEI 19.09.02684.0011790/2021-22 / pg. 95

Anexo II - Autenticação da Mesa da Assembleia Geral Extraordinária realizada em 09 de janeiro de 2017.

Presidente da Mesa — Secretário da Mesa

"ESTATUTO SOCIAL DA STEFANINI RAFAEL SEGURANÇA E DEFESA S.A.

CAPÍTULO I - Da Denominação, Sede, Prazo de Duração e Objeto Social

Artigo 1º - A "**STEFANINI RAFAEL SEGURANÇA E DEFESA S.A.**" é uma sociedade anônima de capital fechado regida pelo presente estatuto e pelas disposições legais que lhe forem aplicáveis.

Artigo 2º - A Companhia tem sede na Avenida Eusébio Matoso, 1.375, 8º. Andar, salas 801 e 802, Butantã, na cidade de São Paulo, Estado de São Paulo, CEP 05423-905, podendo, nos termos do Artigo 16 abaixo, abrir filiais, agências, escritórios ou sucursais em qualquer parte do país ou no exterior.

Artigo 3º - A Companhia tem prazo de duração indeterminado.

Artigo 4º - A Companhia tem por objeto (i) a prestação de serviços de tecnologia da informação, incluindo consultoria, assessoria, suporte técnico em informática, assistência técnica e transferência de tecnologia aplicados à área de defesa e segurança, incluindo a elaboração de projetos, pesquisa, desenvolvimento e inovação tecnológicos; (ii) o desenvolvimento de soluções de automação industrial, softwares e sistemas de defesa e de inteligência, incluindo o desenvolvimento de sistemas de comando e de controle cibernéticos; (iii) o licenciamento de software próprio ou de terceiros customizáveis ou não; (iv) a aquisição e processamento de imagens; (v) a importação, a exportação e o comércio de produtos e/ou serviços relacionados às atividades acima descritas; e (vi) a participação em outras sociedades de qualquer tipo societário, como sócia ou acionista.

CAPÍTULO II - Do Capital Social e das Ações

Artigo 5º - O capital social da Companhia, totalmente subscrito, é de R$4.772.782,00 (quatro milhões, setecentos e setenta e dois mil, setecentos e oitenta e dois reais), dividido em 4.772.782 (quatro milhões, setecentas e setenta e duas mil, setecentas e oitenta e duas) ações, sendo 2.386.391 (dois milhões, trezentas e oitenta e seis mil, trezentas e noventa e uma) ações ordinárias e 2.386.391 (dois milhões, trezentas e oitenta e seis mil, trezentas e noventa e uma) ações preferenciais, todas nominativas e sem valor nominal.

Parágrafo 1º - A ação é indivisível em relação à Companhia. Quando a ação pertencer a mais de uma pessoa, os direitos a ela conferidos serão exercidos pelo representante do condomínio.

Parágrafo 2º - As ações não serão representadas por cautelas, presumindo-se a respectiva propriedade pela inscrição do nome do acionista no livro de registro de ações nominativas.

Anexo Contrato Social (0165188) SEI 19.09.02684.0011790/2021-22 / pg. 96

JUCESP
24 02 17

Artigo 6º - Cada ação ordinária corresponde um voto nas deliberações das Assembleias Gerais.

Artigo 7º - As ações preferenciais não terão direito a voto nas deliberações das Assembleias Gerais, exceto nas hipóteses previstas em lei, neste Estatuto Social e em Acordo de Acionistas arquivado na sede da Companhia e terão os seguintes direitos e vantagens:

(a) outorgarão aos seus titulares prioridade no reembolso do capital, sem prêmio, nos termos do artigo 17, parágrafo II, da Lei nº 6.404/76; e

(b) serão automaticamente conversíveis em igual número de ações ordinárias nominativas e sem valor nominal de emissão da Companhia, nos termos previstos em Acordo de Acionistas arquivado na sede da Companhia.

Artigo 8º - Todas as ações participarão, em igualdade de condições, na distribuição de dividendos pela Companhia ou de qualquer outra forma de pagamento de remuneração aos acionistas.

Parágrafo único - É assegurado direito de preferência aos acionistas para subscrição dos aumentos de capital da Companhia, na proporção do número de ações que possuírem, conforme legislação aplicável e respeitado o Acordo de Acionistas arquivado na sede da Companhia.

Artigo 9º - Nos casos de reembolso de ações, previstos em lei, o valor de reembolso corresponderá ao valor do patrimônio líquido das ações, de acordo com o último balanço aprovado pela Assembleia Geral, segundo os critérios de avaliação do ativo e do passivo fixados na Lei nº 6.404/76 e com os princípios contábeis geralmente aceitos.

CAPÍTULO III - Das Assembleias Gerais

Artigo 10 - As Assembleias Gerais da Companhia serão ordinárias ou extraordinárias, realizando-se, ordinariamente, nos quatro primeiros meses seguintes ao encerramento do exercício social, de acordo com o artigo 132 da Lei nº 6.404/76; e extraordinariamente, sempre que necessário.

Parágrafo 1° - As Assembleias Gerais serão convocadas por qualquer Conselheiro ou por qualquer Acionista, nos casos previstos em lei, neste Estatuto ou no Acordo de Acionistas arquivado na sede da Companhia.

Parágrafo 2° - As Assembleias Gerais serão presididas pelo acionista escolhido por maioria de votos dos presentes e secretariadas por quem o presidente da Assembleia indicar.

Parágrafo 3° - O presidente da Assembleia Geral deverá observar e fazer cumprir as disposições de Acordos de Acionistas arquivados na sede da Companhia, não permitindo que se computem os votos proferidos em contrariedade com o conteúdo de tais acordos.

Parágrafo 4° - As Assembleias Gerais serão instaladas, (i) em primeira convocação, com a presença de acionistas representando, pelo menos, 90% (noventa por cento) do capital social votante da Companhia e, (ii) em segunda convocação, com a presença de acionistas representando, pelo

Anexo Contrato Social (0165188) SEI 19.09.02684.0011790/2021-22 / pg. 97

JUCESP
24 02 17

menos, 60% (sessenta por cento) do capital social votante da Companhia, exceto se a ordem do dia contemplar as matérias listadas no Artigo 11, Parágrafo 1º, deste Estatuto Social (neste caso, o quórum de instalação em segunda convocação também será de, pelo menos, 90% (noventa por cento) do capital social votante da Companhia).

Parágrafo 5º - Só poderão tomar parte e votar na Assembleia Geral os acionistas cujas ações estejam inscritas em seu nome, no registro competente, até 3 (três) dias antes da data marcada para a sua realização.

Artigo 11 - As deliberações da Assembleia Geral, ressalvadas as hipóteses especiais previstas em lei e em Acordo de Acionistas arquivado na sede da Companhia, serão tomadas por maioria de votos dos presentes, não se computando os votos em branco.

Parágrafo 1º - Sem prejuízo do disposto em lei e em Acordo de Acionistas arquivado na sede da Companhia, as decisões sobre as seguintes matérias dependerão da aprovação de acionistas representando mais de 90% (noventa por cento) do capital social votante da Companhia:

(a) modificação do presente Estatuto Social;

(b) aumento ou redução do capital social da Companhia, seja por subscrição, cancelamento, resgate de ações, criação de nova classe de ações ou alteração das características das ações existentes;

(c) modificação do objeto social da Companhia;

(d) aprovação de qualquer alteração material ou cessação dos negócios da Companhia;

(e) eleição e/ou destituição de membros do Conselho de Administração;

(f) definição da remuneração dos membros do Conselho de Administração e da Diretoria da Companhia;

(g) aprovação do relatório da administração e das demonstrações financeiras da Companhia;

(h) declaração ou pagamento de dividendos ou distribuição de lucros pela Companhia aos seus acionistas (observado a legislação aplicável e o Capítulo VI do presente Estatuto Social), incluindo o pagamento de juros sobre capital próprio, bem como quaisquer pagamentos decorrentes de resgates, amortizações, recompra de ações ou restituição de capital;

(i) aprovação de operações de incorporação, fusão, cisão ou qualquer outro tipo de reestruturação societária envolvendo a Companhia ou a transformação da Companhia em outro tipo societário;

(j) constituição de subsidiárias ou aquisição de participação em outras sociedades pela Companhia;

(k) aprovação de oferta pública de valores mobiliários da Companhia; e

(l) liquidação, dissolução, extinção, requerimento de recuperação, judicial ou extrajudicial, e/ou o reconhecimento da falência da Companhia.

Artigo 12 - As deliberações da Assembleia Geral serão válidas somente se tomadas em conformidade com as disposições da Lei nº 6.404/76, deste Estatuto Social e de Acordo de Acionistas arquivado na sede da Companhia.

Anexo Contrato Social (0165188) SEI 19.09.02684.0011790/2021-22 / pg. 98

CAPÍTULO IV - Da Administração

Seção I - Disposições Gerais

Artigo 13 - A Companhia será administrada por um Conselho de Administração e por uma Diretoria.

Parágrafo 1º - A investidura dos administradores da Companhia nos seus cargos far-se-á por termo lavrado em livro próprio, assinado pelo administrador empossado, dispensada qualquer garantia de gestão.

Parágrafo 2º - Os administradores permanecerão em seus cargos até a posse de seus substitutos, exceto se de outra forma for deliberado (i) pela Assembleia Geral, em relação aos membros do Conselho de Administração, ou (ii) pelo Conselho de Administração, em relação aos Diretores.

Parágrafo 3º - A Assembleia Geral fixará um limite de remuneração global anual para distribuição entre os administradores.

Seção II – Conselho de Administração

Artigo 14 - O Conselho de Administração é composto de 5 (cinco) membros, pessoas naturais, acionistas ou não, residentes no País ou no exterior, eleitos pela Assembleia Geral, com mandato de 3 (três) anos, permitida a reeleição.

Parágrafo 1º - O Presidente do Conselho de Administração será eleito pela maioria dos membros deste Conselho e não terá voto de desempate.

Parágrafo 2º - No caso de renúncia, falecimento ou incapacidade de qualquer membro do Conselho de Administração, deverá ser convocada Assembleia Geral para eleição e preenchimento do respectivo cargo, devendo o membro substituto completar o mandato do conselheiro substituído.

Artigo 15 - O Conselho de Administração reunir-se-á sempre que necessário, sendo pelo menos 1 (uma) vez por mês, conforme agenda aprovada na primeira reunião do ano.

Parágrafo 1º - A convocação para as reuniões do Conselho de Administração poderá ser feita por qualquer Conselheiro. Referida convocação deverá ser enviada aos Conselheiros com antecedência mínima de (i) 10 (dez) dias, para primeira convocação, e (ii) 5 (cinco) dias para segunda convocação, e deverá indicar com precisão o local da reunião, a ordem do dia e estar acompanhada dos documentos relacionados aos assuntos a serem discutidos. A convocação será dispensada para as reuniões do Conselho de Administração em que todos os seus membros estiverem presentes. Nenhum negócio ou matéria poderá ser tratado ou aprovado em reunião cuja ordem do dia não tenha descrito tal assunto, a não ser que todos os membros do Conselho de Administração estejam presentes em tal reunião.

Parágrafo 2º - Os trabalhos das reuniões do Conselho de Administração serão dirigidos por mesa composta pelo Presidente do Conselho de Administração e pelo Secretário da Companhia, cujas funções e mandato são previstas no Artigo 17, abaixo.

Anexo Contrato Social (0165188) SEI 19.09.02684.0011790/2021-22 / pg. 99

Parágrafo 3º - As reuniões do Conselho de Administração serão instaladas com a presença de, pelo menos, 4 (quatro) membros.

Parágrafo 4º - Os membros do Conselho de Administração serão considerados regularmente presentes nas reuniões do órgão quando (i) participarem por meio de videoconferência, conferência telefônica ou qualquer outro sistema de comunicação que possibilite conexão simultânea, ou (ii) enviarem os seus votos por escrito, através de e-mail, fax, carta ou telegrama, à Companhia, em atenção do Presidente do Conselho de Administração no mesmo dia da reunião.

Parágrafo 5º - As deliberações das reuniões do Conselho de Administração serão consignadas em ata lavrada em livro próprio e assinada por todos os membros presentes. A ata assinada será prova *"prima facie"* dos procedimentos e deliberações do Conselho de Administração. Serão arquivadas no registro do comércio e publicadas as atas que contiverem deliberação destinada a produzir efeitos perante terceiros.

Parágrafo 6º - O presidente da reunião do Conselho de Administração deverá observar e fazer cumprir as disposições de Acordos de Acionistas arquivados na sede da Companhia, não permitindo que se computem os votos proferidos em contrariedade com o conteúdo de tais acordos.

Artigo 16 - Sem prejuízo das demais matérias que lhe sejam atribuídas por lei e respeitadas as demais disposições de Acordo de Acionistas arquivado na sede da Companhia, compete privativamente ao Conselho de Administração, dentro de suas atribuições legais e estatutárias, deliberar a respeito das matérias elencadas abaixo, sendo que referidas deliberações dependerão de voto afirmativo de, pelo menos, 4 (quatro) Conselheiros:

(a) aprovação de quaisquer propostas a serem submetidas à Assembleia Geral, relacionadas aos assuntos descritos no Artigo 11, Parágrafo 1º, acima;

(b) aprovação do plano de negócios e orçamento anual da Companhia, bem como suas respectivas modificações;

(c) aprovação do plano comercial da Companhia e suas respectivas modificações;

(d) eleição e/ou destituição de membros da Diretoria da Companhia;

(e) escolha e/ou destituição dos auditores independentes da Companhia;

(f) decisão sobre a forma de financiamento da Companhia;

(g) contratação de empréstimos, financiamentos ou qualquer outra forma de endividamento pela Companhia, que não estejam expressamente previstos no plano de negócios e que envolvam valores acima de R$100.000,00;

(h) celebração de contratos ou operações relevantes pela Companhia que não estejam no curso normal dos negócios ou que envolvam valores acima de R$1.000.000,00 ou que possuam prazo de duração de mais de 12 meses;

(i) início de tratativas ou a realização de acordo de qualquer procedimento judicial, administrativo ou arbitral envolvendo a Companhia bem como o pagamento de qualquer reclamação/ação envolvendo a Companhia, em cada caso, envolvendo valores superiores a R$ 100.000,00;

Anexo Contrato Social (0165188) SEI 19.09.02684.0011790/2021-22 / pg. 100

(j) concessão de garantias em benefício de terceiros;

(k) abertura e/ou encerramento pela Companhia de filiais, agências, escritórios ou sucursais no país ou no exterior;

(l) realização de investimentos (Capex) pela Companhia, não contemplados no plano de negócios e envolvendo valores acima de R$ 100.000,00;

(m) aprovação do código de conduta da Companhia;

(n) aprovação de quaisquer operações entre a Companhia e partes relacionadas;

(o) transferência, disposição ou oneração de bens do ativo permanente pela Companhia;

(p) transferência, cessão ou oneração de ativos de propriedade intelectual pela Companhia;

(q) aprovação das matérias acima com relação às subsidiárias da Companhia, incluindo manifestação de voto em seus respectivos atos societários; e

(r) aprovação das matérias descritas no Artigo 11, Parágrafo 1º, acima com relação às subsidiárias da Companhia, incluindo manifestação de voto em seus respectivos atos societários.

Parágrafo único – Nos demais casos não previstos no caput acima ou em acordos celebrados entre os acionistas, o Conselho de Administração deliberará por maioria de votos dos seus membros.

Artigo 17 – O Conselho de Administração deverá eleger um Secretário da Companhia. O mandato do Secretário da Companhia será renovado anualmente ou em outra periodicidade conforme venha a ser determinado pelo Conselho de Administração.

Parágrafo único – O Secretário da Companhia deverá:

(a) preparar, coordenar e manter o calendário de reuniões do Conselho de Administração;

(b) atuar como secretário nas reuniões do Conselho de Administração e auxiliar o Presidente do Conselho de Administração em quaisquer assuntos a estas relacionados; e

(c) preparar e circular as atas de reunião do Conselho de Administração para todos os Conselheiros, bem como preparar quaisquer traduções de tal documento para o inglês.

Seção III – Diretoria

Artigo 18 – A Diretoria é composta por 2 (dois) ou mais membros, todos residentes no País, com prazo de gestão de 3 (três) anos, permitida a reeleição, sendo 1 (um) Diretor Presidentee 1 (um) Diretor de Operações ou Diretor Técnico. Os demais Diretores, se houver, terão a designação a eles atribuída pelo Conselho de Administração.

Anexo Contrato Social (0165188) SEI 19.09.02684.0011790/2021-22 / pg. 101

Parágrafo 1º - A Diretoria é o órgão executivo e de representação da Companhia, cabendo-lhe assegurar o funcionamento regular desta, tendo poderes para praticar todos e quaisquer atos relativos aos fins sociais, exceto aqueles que por lei ou pelo presente Estatuto Social dependam de prévia aprovação do Conselho de Administração ou da Assembleia Geral.

Parágrafo 2º - A Diretoria não é um órgão colegiado e cada Diretor cumprirá sua função exclusivamente dentro de suas atribuições e responsabilidades, conforme as diretrizes do Conselho de Administração, o presente Estatuto Social e Acordo de Acionistas arquivado na sede da Companhia.

Artigo 19 - A Companhia considerar-se-á obrigada quando representada:

(a) por 2 (dois) Diretores em conjunto;

(b) por 1 (um) Diretor, em conjunto com 1 (um) procurador com poderes específicos, nos termos do Parágrafo único abaixo;

(c) por 1 (um) ou mais procuradores com poderes específicos, nos termos do Parágrafo 1º abaixo; ou

(d) por qualquer Diretor ou procurador, para a prática de atos que envolvam exclusivamente a representação da Companhia em processos judiciais e/ou administrativos.

Parágrafo 1º - As procurações serão sempre outorgadas em nome da Companhia por 2 (dois) Diretores em conjunto, especificação os poderes outorgados e terão prazo de validade limitado ao máximo de 1 (um) ano, exceto pelas procurações *ad judicia*, que podem ter prazo de duração superior a 1 (um) ano ou tempo indeterminado.

Parágrafo 2º - É vedado aos Diretores concederem fianças, avais ou outras garantias em nome da Companhia, bem como contrair obrigações de qualquer natureza em favor de terceiros em negócios estranhos ao objeto social, sem a prévia e expressa autorização da Assembleia Gera ou Conselho de Administração, conforme o caso, sob pena de responderem pessoalmente pela infração desta cláusula.

CAPÍTULO V - Do Conselho Fiscal

Artigo 20 - O Conselho Fiscal somente será instalado a pedido dos acionistas e possuirá as competências, responsabilidades e deveres, tudo conforme o disposto na Lei nº 6.404/76.

Artigo 21 - Caso solicitado seu funcionamento, os acionistas deverão eleger 3 (três) membros efetivos e igual número de suplentes para compor o Conselho Fiscal, observado o disposto na Lei nº 6.404/76; cada período de funcionamento do Conselho Fiscal terminará na primeira Assembleia Geral Ordinária após sua instalação.

Artigo 22 - A remuneração dos Conselheiros Fiscais será determinada pela Assembleia Geral que os eleger.

Anexo Contrato Social (0165188) SEI 19.09.02684.0011790/2021-22 / pg. 102

CAPÍTULO VI - Do Exercício Social e Distribuição de Lucros

Artigo 23 - O exercício social terminará no dia 31 de dezembro de cada ano, quando serão elaboradas as demonstrações financeiras previstas na legislação aplicável.

Artigo 24 – Juntamente com as demonstrações financeiras do exercício social, o Conselho de Administração deverá apresentar à Assembleia Geral uma proposta para a destinação do lucro líquido da Companhia, de acordo com o estabelecido neste Estatuto Social e na legislação aplicável.

Artigo 25 - Do lucro líquido apurado pela Companhia, serão destinados:

a) 5% (cinco por cento), para a Reserva Legal, até atingir 20% (vinte por cento) do capital social; e

b) 25% (vinte e cinco por cento), para distribuição aos acionistas a título de dividendo obrigatório.

Parágrafo 1º - O dividendo previsto neste artigo não será obrigatório no exercício social em que a administração informar à Assembleia Geral não ser ele compatível com a situação financeira da Companhia. O Conselho Fiscal, se em funcionamento, deverá dar parecer sobre essa informação. Os lucros que assim deixarem de ser distribuídos serão registrados como reserva especial e, se não absorvidos por prejuízos em exercícios subsequentes, deverão ser pagos como dividendos assim que o permitir a situação financeira da Companhia.

Parágrafo 2º - O saldo do lucro líquido terá a destinação que a Assembleia Geral determinar, podendo ser transferido para reserva de lucros, cujos saldos, somados, não poderão ultrapassar o capital social; atingindo esse limite, a Assembleia Geral deliberará sobre a aplicação do excesso em aumento do capital social ou na distribuição de dividendos.

Parágrafo 3º - A Assembleia Geral poderá, desde que não haja oposição de qualquer acionista presente, deliberar a distribuição de dividendo inferior ao previsto neste artigo ou a retenção de todo o lucro.

Artigo 26 - A Companhia, por deliberação da Assembleia Geral, poderá levantar balancetes intermediários, e pagar dividendos de acordo com os lucros apurados nesses balancetes.

Artigo 27 - A Companhia poderá remunerar os acionistas mediante pagamento de juros sobre capital próprio, na forma aprovada pela Assembleia Geral, a qual fixará o montante e data de pagamento, sendo que os valores correspondentes aos juros sobre capital próprio poderão ser imputados ao dividendo obrigatório.

CAPÍTULO VII - Da Liquidação

Artigo 28 - A Companhia entrará em liquidação nos casos legais, cabendo à Assembleia Geral determinar o modo de liquidação e nomear o liquidante que deverá atuar nesse período.

Anexo Contrato Social (0165188) SEI 19.09.02684.0011790/2021-22 / pg. 103

JUCESP
24 02 17

CAPÍTULO VIII - Das Disposições Finais

Artigo 29 - A Companhia e seus administradores observarão Acordo de Acionistas arquivado em sua sede, sendo expressamente vedado aos integrantes da mesa diretora da Assembleia Geral ou do Conselho de Administração acatar ou registrar qualquer declaração de voto de qualquer acionista signatário ou administrador vinculado a tais acordos de acionistas que for proferida em desacordo com o que tiver sido ajustado em referidos acordos, sendo também expressamente vedado à Companhia aceitar e proceder à transferência de ações e/ou direitos de subscrição de ações ou outros valores mobiliários em descumprimento ao previsto em tais acordos. Da mesma forma, os administradores da Companhia ficam proibidos de praticar qualquer ato em desconformidade com os acordos de acionistas arquivados na sede da Companhia.

CAPÍTULO IX - Da Lei Aplicável, Jurisdição e Arbitragem

Artigo 30 - Este Estatuto Social será regido e interpretado de acordo com as Leis da República Federativa do Brasil.

Artigo 31 - Os conflitos e controvérsias envolvendo a Companhia e qualquer de seus acionistas serão dirimidos por arbitragem na cidade de São Paulo, Estado de São Paulo, nos termos previstos em Acordo de Acionistas arquivado na sede da Companhia.

Artigo 32 - Os acionistas permanecem com o direito de requerer no juízo comum competente as medidas judiciais que visem à obtenção de medidas cautelares para proteção ou salvaguarda de direitos ou de cunho preparatório previamente à instauração do Tribunal de Arbitragem sem que isso seja interpretado como uma renúncia à arbitragem. Para o exercício das citadas tutelas jurisdicionais os Acionistas elegem o Foro Central da Comarca da Capital do estado de São Paulo, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

Artigo 33 - O presente Estatuto Social entra em vigor na data de sua aprovação pela Assembleia Geral."

Advogado:

Roberto Lourenço Bellizzo
OAB/SP n.º 147.215

Anexo Contrato Social (0165188) SEI 19.09.02684.0011790/2021-22 / pg. 104

TERMO DE POSSE

Nesta data, eu, **WANDER MARQUES CUNHA**, [redacted] posse do cargo de Membro do Conselho de Administração da **STF PROJETOS E SERVIÇOS DE TECNOLOGIA DE DEFESA S.A.** ("Companhia"), conforme eleições aprovadas em Assembleia Geral Extraordinária da Companhia, datada de 09 de janeiro de 2017.

Declaro, para os devidos fins, que o endereço acima é o endereço no qual receberei as citações e intimações em processos administrativos e judiciais relativos a atos de minha gestão na Companhia.

Declaro, ainda, sob as penas da lei, que não estou incurso em quaisquer crimes previstos em Lei ou restrições legais, que possam me impedir de exercer atividades empresariais e que não estou impedido de exercer a administração da Companhia, por lei especial, ou em virtude de condenação criminal ou por me encontrar sob os efeitos dela, a pena que vede, ainda que temporariamente, o acesso a cargos públicos; ou por crime falimentar, de prevaricação, peita ou suborno, concussão, peculato; ou contra a economia popular, contra o sistema financeiro nacional, contra as normas de defesa da concorrência, contra as relações de consumo, fé pública, ou a propriedade.

São Paulo, 09 de janeiro de 2016.

Wander M. Cunha

WANDER MARQUES CUNHA
MEMBRO DO CONSELHO DE ADMINISTRAÇÃO

INVESTITURE TERM

On the date hereof, I, **WANDER MARQUES CUNHA**, [redacted] assume the position Member of the Board of Directors of **STF PROJETOS E SERVIÇOS DE TECNOLOGIA DE DEFESA S.A.** ("Company"), as per the elections approved on the Shareholders Meeting held on January 09, 2017.

I declare, for all the legal purposes, that the aforementioned address is the one in which I shall receive any summons and subpoenas in law and administrative suits regarding my managing acts on the Company.

I also declare, under the penalties of the law, that I am not convicted of any of the felonies set forth in the law or have no current restrictions that can impede me same to exert the business activities or management of the Company, by law or by virtue of criminal conviction or am penalized, even temporarily to be prevented to assume public offices, or bankruptcy felonies, prevarication, bribery, graft, embezzlement, or felonies against popular economy, national financial system, anti-trust crimes, public faith or crimes against property.

São Paulo, January 09, 2016.

Wander M. Cunha

[signature]
BY:
MEMBER OF BOARD OF DIRECTORS

Anexo Contrato Social (0165188) SEI 19.09.02684.0011790/2021-22 / pg. 105

TERMO DE POSSE

Nesta data, eu, **MARCOS PEREIRA DE ALMEIDA,** [redacted] posse do cargo de Membro do Conselho de Administração da **STF PROJETOS E SERVIÇOS DE TECNOLOGIA DE DEFESA S.A.** ("Companhia"), conforme eleições aprovadas em Assembleia Geral Extraordinária da Companhia, datada de 09 de janeiro de 2017.

Declaro, para os devidos fins, que o endereço acima é o endereço no qual receberei as citações e intimações em processos administrativos e judiciais relativos a atos de minha gestão na Companhia.

Declaro, ainda, sob as penas da lei, que não estou incurso em quaisquer crimes previstos em Lei ou restrições legais, que possam me impedir de exercer atividades empresariais e que não estou impedido de exercer a administração da Companhia, por lei especial, ou em virtude de condenação criminal ou por me encontrar sob os efeitos dela, a pena que vede, ainda que temporariamente, o acesso a cargos públicos; ou por crime falimentar, de prevaricação, peita ou suborno, concussão, peculato; ou contra a economia popular, contra o sistema financeiro nacional, contra as normas de defesa da concorrência, contra as relações de consumo, fé pública, ou a propriedade.

São Paulo, 09 de janeiro de 2016.

MARCOS PEREIRA DE ALMEIDA
MEMBRO DO CONSELHO DE ADMINISTRAÇÃO

INVESTITURE TERM

On the date hereof, I, **MARCOS PEREIRA DE ALMEIDA,** [redacted] position Member of the Board of Directors of **STF PROJETOS E SERVIÇOS DE TECNOLOGIA DE DEFESA S.A.** ("Company"), as per the elections approved on the Shareholders Meeting held on January 09, 2017.

I declare, for all the legal purposes, that the aforementioned address is the one in which I shall receive any summons and subpoenas in law and administrative suits regarding my managing acts on the Company.

I also declare, under the penalties of the law, that I am not convicted of any of the felonies set forth in the law or have no current restrictions that can impede me same to exert the business activities or management of the Company, by law or by virtue of criminal conviction or am penalized, even temporarily to be prevented to assume public offices, or bankruptcy felonies, prevarication, bribery, graft, embezzlement, or felonies against popular economy, national financial system, anti-trust crimes, public faith or crimes against property.

São Paulo, January 09, 2016.

[signature]
BY:
MEMBER OF BOARD OF DIRECTORS

Anexo Contrato Social (0165188) SEI 19.09.02684.0011790/2021-22 / pg. 106

TERMO DE POSSE

Nesta data, eu, **MARCO ANTÔNIO SILVA STEFANINI**, [redacted] tomo posse do cargo de Membro do Conselho de Administração da **STF PROJETOS E SERVIÇOS DE TECNOLOGIA DE DEFESA S.A.** ("Companhia"), conforme eleições aprovadas em Assembleia Geral Extraordinária da Companhia, datada de 09 de janeiro de 2017.

Declaro, para os devidos fins, que o endereço acima é o endereço no qual receberei as citações e intimações em processos administrativos e judiciais relativos a atos de minha gestão na Companhia.

Declaro, ainda, sob as penas da lei, que não estou incurso em quaisquer crimes previstos em Lei ou restrições legais, que possam me impedir de exercer atividades empresariais e que não estou impedido de exercer a administração da Companhia, por lei especial, ou em virtude de condenação criminal ou por me encontrar sob os efeitos dela, a pena que vede, ainda que temporariamente, o acesso a cargos públicos; ou por crime falimentar, de prevaricação, peita ou suborno, concussão, peculato; ou contra a economia popular, contra o sistema financeiro nacional, contra as normas de defesa da concorrência, contra as relações de consumo, fé pública, ou a propriedade.

São Paulo, 09 de janeiro de 2016.

Marco Antonio Stefanini

MARCO ANTÔNIO SILVA STEFANINI
MEMBRO DO CONSELHO DE ADMINISTRAÇÃO

INVESTITURE TERM

On the date hereof, I, **MARCO ANTÔNIO SILVA STEFANINI**, [redacted] assume the position Member of the Board of Directors of **STF PROJETOS E SERVIÇOS DE TECNOLOGIA DE DEFESA S.A.** ("Company"), as per the elections approved on the Shareholders Meeting held on January 09, 2017.

I declare, for all the legal purposes, that the aforementioned address is the one in which I shall receive any summons and subpoenas in law and administrative suits regarding my managing acts on the Company.

I also declare, under the penalties of the law, that I am not convicted of any of the felonies set forth in the law or have no current restrictions that can impede me same to exert the business activities or management of the Company, by law or by virtue of criminal conviction or am penalized, even temporarily to be prevented to assume public offices, or bankruptcy felonies, prevarication, bribery, graft, embezzlement, or felonies against popular economy, national financial system, anti-trust crimes, public faith or crimes against property.

São Paulo, January 09, 2016.

[signature]
BY:
MEMBER OF BOARD OF DIRECTORS

Anexo Contrato Social (0165188) SEI 19.09.02684.0011790/2021-22 / pg. 107

TERMO DE POSSE

Nesta data, eu, **AVI KRENGEL**, cidadão [redacted] Conselho de Administração da **STEFANINI RAFAEL SEGURANÇA E DEFESA S.A.** ("Companhia"), conforme eleições aprovadas em Assembleia Geral Extraordinária da Companhia, datada de 09 de janeiro de 2017.

Declaro, para os devidos fins, que o endereço acima é o endereço no qual receberei as citações e intimações em processos administrativos e judiciais relativos a atos de minha gestão na Companhia.

Declaro, ainda, sob as penas da lei, que não estou incurso em quaisquer crimes previstos em Lei ou restrições legais, que possam me impedir de exercer atividades empresariais e que não estou impedido de exercer a administração da Companhia, por lei especial, ou em virtude de condenação criminal ou por me encontrar sob os efeitos dela, a pena que vede, ainda que temporariamente, o acesso a cargos públicos; ou por crime falimentar, de prevaricação, peita ou suborno, concussão, peculato; ou contra a economia popular, contra o sistema financeiro nacional, contra as normas de defesa da concorrência, contra as relações de consumo, fé pública, ou a propriedade.

São Paulo, 09 de janeiro de 2017.

INVESTITURE TERM

On the date hereof, I, **AVI KRENGEL**, [redacted] Member of the Board of Directors of **STEFANINI RAFAEL SEGURANÇA E DEFESA S.A.** ("Company"), as per the elections approved on the Shareholders Meeting held on January 09, 2017.

I declare, for all the legal purposes, that the aforementioned address is the one in which I shall receive any summons and subpoenas in law and administrative suits regarding my managing acts on the Company.

I also declare, under the penalties of the law, that I am not convicted of any of the felonies set forth in the law or have no current restrictions that can impede me same to exert the business activities or management of the Company, by law or by virtue of criminal conviction or am penalized, even temporarily to be prevented to assume public offices, or bankruptcy felonies, prevarication, bribery, graft, embezzlement, or felonies against popular economy, national financial system, anti-trust crimes, public faith or crimes against property.

São Paulo, January 09, 2017.

AVI KRENGEL
MEMBRO DO CONSELHO DE ADMINISTRAÇÃO / MEMBER OF BOARD OF DIRECTORS

21º TABELIÃO DE NOTAS DE SÃO PAULO
Rua Libero Badaro 386 – 2º andar
AUTENTICAÇÃO
Autentico a presente cópia extraída destas notas conforme a original apresentado, dou fé.
08 FEV 2017
Rodrigo Fernando Baez
Válido somente com o selo de autenticidade
AUT. R$ 3,30
AUTENTICAÇÃO
1084AW0124825

Anexo Contrato Social (0165188) SEI 19.09.02684.0011790/2021-22 / pg. 108

JUCESP

JUCESP PROTOCOLO
0.165.094/18-7

STEFANINI RAFAEL SEGURANÇA E DEFES
CNPJ/MF nº 24.691.488/0001-09
NIRE 35.300.492.650

ATA DA ASSEMBLEIA GERAL EXTRAORDINÁRIA REALIZADA EM 30 DE NOVEMBRO DE 2017

I. Data, Hora e Local: Realizada no dia 30 de novembro de 2017, às 10h, na Avenida Eusébio Matoso, 1.375, 8º Andar, cidade e Estado de São Paulo, CEP 05423-905.

II. Convocação e Presença: Dispensada a publicação de editais de convocação, nos termos do disposto no Artigo 124, § 4º da Lei nº 6.404/76 ("Lei das S.A."), tendo em vista a presença da totalidade dos acionistas da Companhia, conforme assinaturas lançadas no "Livro de Presença de Acionistas".

III. Composição da Mesa: Sr. Marco Antônio Silva Stefanini (Presidente) e Sr. Marcos Pereira de Almeida (Secretário).

IV. Ordem do dia: Deliberar sobre a eleição de novo membro do Conselho de Administração, ante a renúncia de um de seus membros.

V. Deliberações: Após análise e discussões sobre as matérias constantes da ordem do dia, decidiu-se, por unanimidade e sem quaisquer restrições:

(1) tomar ciência da renúncia do Sr. Wander Marques Cunha, nesta data, ao cargo de membro do Conselho de Administração da Companhia, ao qual prestam os devidos agradecimentos pelos serviços prestados em prol da Companhia.

(2) aprovar, ante a renúncia do Sr. Wander Marques Cunha, a eleição para o cargo de membro do Conselho de Administração, por um mandato a se encerrar na data da Assembleia Geral Ordinária da Companhia a ser realizada em 2019, do Sr. **Ailtom Barberino do Nascimento Filho,** [redacted]

O membro do Conselho de Administração ora eleito declara, nesta data, sob as penas da lei, que não está impedido, por lei especial, de exercer a administração de sociedades, nem condenado ou sob efeitos de condenação, a pena que vede, ainda que temporariamente, o acesso a cargos públicos; ou por crime falimentar, de prevaricação, peita ou suborno, concussão, peculato; ou contra a economia popular, a fé pública ou a propriedade, bem como cumprem com os demais requisitos da Lei nº 6.404/76. Dessa forma, o membro do Conselho de Administração ora eleito toma posse em seus cargos, mediante a assinatura do respectivo Termo de Posse no Livro de Atas de Reunião do Conselho de Administração.

(3) autorizar a Diretoria da Companhia proceder à atualização dos registros e anotações junto aos órgãos públicos competentes para que conste a transformação da Sociedade em sociedade anônima, informando sua nova denominação social, bem como aprovar a lavratura e publicação da presente Ata sob a forma de sumário dos fatos ocorridos, nos termos dos §§ 1º e 3º do Artigo 130 da LSA.

VI. Encerramento: Nada mais havendo a tratar e, como ninguém mais desejava fazer uso da palavra, foram encerrados os trabalhos e a presente ata foi lavrada, tendo sido lida, achada conforme e assinada pelos presentes. Mesa: **Marco Antônio Silva Stefanini** (presidente), **Marcos Pereira de Almeida** (secretário). Acionistas presentes: **Stefanini Participações S.A.**

Anexo Contrato Social (0165188) SEI 19.09.02684.0011790/2021-22 / pg. 109

(p. Marco Antônio Silva Stefanini) e **Rafael Advanced Defense Systems Ltd.** (pp. Fabiano Gallo).

Confere com a original lavrada no livro próprio.

São Paulo (SP), 30 de novembro de 2017.

Marco Antônio Silva Stefanini
Presidente

Marcos Pereira de Almeida
Secretário

(Página de Assinaturas da Ata da Assembleia Geral Extraordinária da Stefanini Rafael Segurança e Defesa S.A., realizada em 30 de novembro de 2017)

SECRETARIA DE DESENVOLVIMENTO ECONÔMICO, CIÊNCIA, TECNOLOGIA E INOVAÇÃO
JUCESP
CERTIFICO O REGISTRO SOB O NÚMERO
FLAVIA R. BRITTO GONÇALVES
SECRETÁRIA GERAL
101.687/18-7
JUCESP
JUCESP
0 1 MAR 2018
SEDE

Anexo Contrato Social (0165188) SEI 19.09.02684.0011790/2021-22 / pg. 110

JUCESP

01 DEZ 17

TERMO DE POSSE

Nesta data, eu, **AILTOM BARBERINO DO NASCIMENTO FILHO**, brasileiro, casado, administrador de empresas, portador da cédula de identidade RG [redacted] como posse do cargo de membro do Conselho de Administração da **STEFANINI RAFAEL SEGURANÇA E DEFESA S.A.**, conforme eleição aprovada em Assembleia Geral Extraordinária da Companhia, datada de 30 de novembro de 2017.

Declaro, para os devidos fins, que o endereço acima é o endereço no qual receberei as citações e intimações em processos administrativos e judiciais relativos a atos de minha gestão na Companhia.

Declaro, ainda, sob as penas da lei, que não estou impedido de exercer a administração da Companhia por lei especial ou em virtude de condenação criminal, ou por se encontrar sob os efeitos dela, a pena que vede, ainda que temporariamente, o acesso a cargos públicos; ou por crime falimentar, de prevaricação, peita ou suborno, concussão, peculato, ou contra a economia popular, contra o sistema financeiro nacional, contra normas de defesa da concorrência, contra as relações de consumo, fé pública, ou a propriedade.

São Paulo, 30 de novembro de 2017.

AILTOM BARBERINO DO NASCIMENTO FILHO
Membro do Conselho de Administração

São Paulo, 30 de novembro de 2017

Em mãos

À

STEFANINI RAFAEL SEGURANÇA E DEFESA S.A.

Prezados Senhores,

Venho, por meio desta, renunciar ao cargo de membro do Conselho de Administração da Stefanini Rafael Segurança e Defesa S.A., sociedade por ações, com sede na cidade de São Paulo, Estado de São Paulo, na Avenida Eusébio Matoso, 1.375, 8º andar, CEP 05423-905, inscrita no CNPJ/MF sob o nº 24.691.488/0001-09 ("Companhia"), em razão do que outorgo à Companhia a mais ampla, plena, rasa, geral, irrevogável e irretratável quitação, por todo o período de gestão, para nada mais reclamar da Companhia, a qualquer tempo ou título.

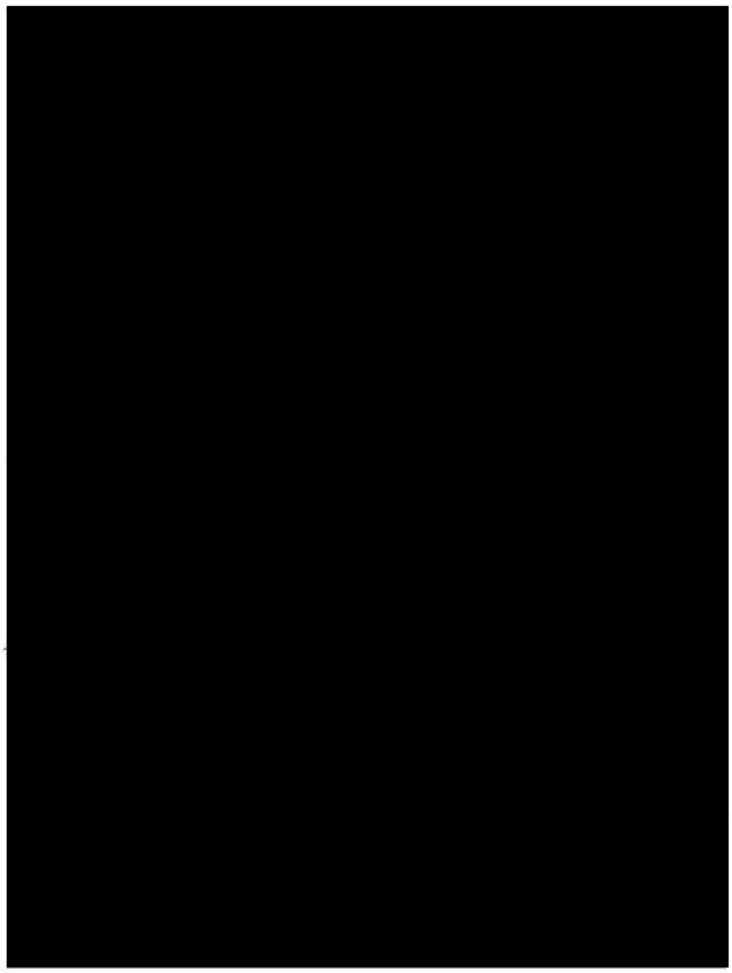
Sem mais,

Atenciosamente,

Wander M. Cunha

Wander Marques Cunha

CARTÓRIO DO 15º TABELIÃO DE NOTAS
Av. Dr. Cardoso de Melo, 1855
(Esq. da R. Funchal) - Tel. 3045-0515/3058-5100
AUTENTICAÇÃO - Autentico a Presente
cópia reprográfica extraída, conforme
original apresentado. Dou fé.
S. Paulo,
22 FEV. 2018
Selo Digital Notarial do Brasil
AUTENTICAÇÃO
1059BBD3590330
VÁLIDO SOMENTE COM O SELO DE AUTENTICIDADE
Wilson Ap... ESCREV... CUSTAS C...



São Paulo, 9 de setembro de 2020.

Nº

ATESTADO DE IDONEIDADE

A quem possa interessar, declaramos para todos os fins e efeitos de direito, que STEFANINI RAFAEL SEGURANCA E DEFESA SA, inscrito(a) no CNPJ/MF sob o nº 24.691.488/0001-09 sediado na AV EUSEBIO MATOSO 1375 AND 8 SL 801 802 - BUTANTA - CEP: 05423-905 - SAO PAULO - SP é nosso(a) Cliente e tem acesso aos nossos produtos financeiros. Informamos, ainda, que nosso(a) Cliente mantém relacionamento comercial conosco desde 08/2019 na Agência 0393 Conta Corrente 12466-4.

Conforme nossos arquivos, declaramos que o Cliente acima qualificado(a) não registra, nesta data, qualquer atraso no pagamento das linhas de crédito concedidas por esta instituição financeira, sendo, portanto, financeiramente idônea até a presente data. Tal declaração é realizada dentro do restrito limite das relações comerciais mantidas até a presente data com nosso(a) cliente acima qualificado(a).

A presente declaração, fornecida para uso exclusivo interno de quem receber essa declaração, não constitui qualquer obrigação e nem comprometimento de nossa parte, bem como não pode ser utilizada ou entendida, sob qualquer circunstância, como garantia bancária emitida por esta instituição.

Atenciosamente,

ITAÚ UNIBANCO S.A.

Rodrigo Reinatti Souza
RG: [redacted]
CPF: [redacted]

Elmo Sadao Iosimura Filho
CPF: [redacted]
RG [redacted]

Anexo Comprovante Bancário (0164282) SEI 19.09.02684.0011790/2021-22 / pg. 114

IBLISS
DIGITAL SECURITY

MINISTÉRIO PÚBLICO
DO ESTADO DA BAHIA

- Proposta Testes de Invasão
14/07/2021 | Validade: 30 dias

A EMPRESA

A IBLISS, empresa especializada em segurança digital, é referência nacional em desenvolvimento e fornecimento de soluções estratégicas para a proteção de negócios e pessoas.
Fundada em São Paulo em 2009 e formada por especialistas e engenheiros certificados com mais de quinze anos de experiência, a iBLISS tem apoiado empresas 100+ da Exame e Fortune 500 em projetos de Segurança da Informação de alta complexidade, gestão de riscos, diagnósticos, adequação, monitoração e prevenção de ameaças digitais.
Por meio de programas estratégicos de proteção orientado aos objetivos de negócio de cada companhia, a abordagem de atuação da iBLISS possibilita a melhoria contínua da maturidade em segurança com redução de custo.

Posicionamento

A transformação digital tem feito com que a segurança tradicional seja levada a uma nova realidade, que deve levar em consideração o atual cenário de ameaças, em que os ataques cibernéticos têm causado uma série de prejuízos às finanças e à imagem da empresa.
Nossa abordagem é baseada no contexto de cada negócio com o objetivo de reduzir custos com a prevenção de incidentes e perdas e dar apoio à tomada de decisão com base em análises técnicas sempre alinhadas à política corporativa e às melhores práticas de segurança.
A iBLISS gerencia e monitora mais de 100 mil ativos por mês, realizando testes de segurança, consultorias, proteção de aplicações e programas de conscientização. Atuamos nos principais segmentos de mercado, atendendo a requisitos de segurança generalistas e regulamentações específicas, como PCI-DSS, SOX, TISS entre outras.

Missão

Por meio de serviços especializados, pesquisa, desenvolvimento e inovação, apoiar a maturidade e o gerenciamento de riscos de nossos clientes, e contribuir para o crescimento do mercado brasileiro em soluções de segurança da informação.

A EMPRESA

IBLISS DIGITAL SECURITY

+60 Clientes	+100.000	+10.000 horas	+12 Anos	+30%
+10 na lista das 100 Maiores Empresas da Exame	Ativos analisados por mês	de testes de segurança por ano	de experiência em Projetos Especiais	Crescimento anual desde 2013

FUNDAÇÃO ABRINQ

Great Place To Work. Certificado 24/02/2020 - 24/02/2021 BRASIL

inovaBra habitat

A EMPRESA

IBLISS DIGITAL SECURITY

Equipe

Formada por profissionais com grande vivência de mercado, nossa equipe possui profundo conhecimento e constante atualização a respeito de técnicas de ataque, novas ameaças e métodos de proteção.
Isso se dá, principalmente, por conta de publicações e participações em comunidades e congressos nacionais e internacionais (DefCon, HITB, OWASP, ToorCon, H2HC, YSTS), além da obtenção de certificações (SANS GIAC, CEH, MCSO, CCNA, CCDA, ITIL, Cobit, ISO 27002, entre outras).

Dados Cadastrais

Razão Social: IBLISS Segurança Digital LTDA.
CNPJ: 10.739.169/0001-11
Endereço: Av. Angélica, 2582 - cj 22 - Higienópolis, São Paulo - SP - Brasil
Representante Legal: Leonardo Cavallari Militelli
E-mail: leonardo.militelli@ibliss.com.br
Ref. Bancárias: Banco Itaú – Ag.: 3052 – C/C: 09668-6

A EMPRESA

IBLISS DIGITAL SECURITY

Empresa com propósito

Programa de responsabilidade social

- Incentivar a navegação saudável
- Inclusão de mulheres em Cyber Segurança

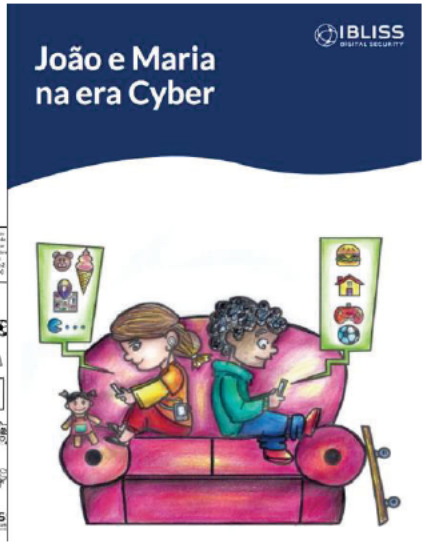
Apoia à comunidade de infosec

- Conferências
- Palestras e colaboração

https://www.ibliss.digital/responsabilidadesocial/

FUNDAÇÃO ABRINQ





NULLBYTE

WOMCY LATAM Women in Cybersecurity

OWASP

Anexo Orçamento 02 (0264287) SEI 19.09.02684.0011790/2021-22 / pg. 119

CLIENTES

Varejo e Indústria

viavarejo · 3 Corações · Ajinomoto · Solar Coca-Cola · atech Grupo Embraer

Financeiro e Meios de Pagamento

Itaú · Bradesco · Safra · Banco Máxima · Honda Serviços Financeiros · Santander · CIP · Banco Paulista · ParanáBanco · stone

Saúde

Hypera pharma · novo nordisk · 4BIO · aliar médicos à frente · db Medicina Diagnóstica

Logística

EMBRAPORT · Brasil Terminal Portuário · S.Magalhães Essemaga · sequoia

Telecom e Tecnologia

Telefônica · TIM · Algar · AUTOPASS · LISTO

Serviços

sodexo · livelo · stix · alelo · CVC · Repom · yandeh · involves · acesso digital

Governo e Associações

CIESP · FIESP · UNINOVE Universidade Nove de Julho · Ministério Público Estado da Bahia

IBLISS DIGITAL SECURITY

Construa seu Programa de Segurança da Informação e Privacidade!

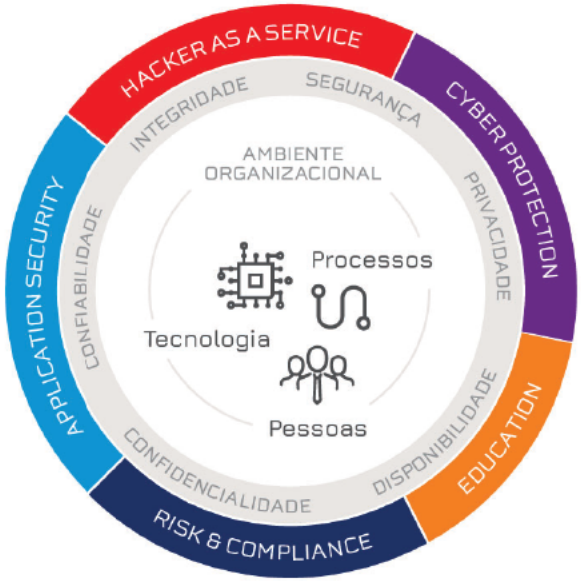


ISO 27001 Certified · GDPR READY · General Data Protection Regulation · LGPD Lei Geral de Proteção de Dados Pessoais · NIST National Institute of Standards and Technology U.S. Department of Commerce · PCI Security Standards Council

OBJETIVO

O objetivo deste trabalho é a realização de serviço de Testes de invasão, proporcionando um melhor direcionamento de seus recursos, através de recomendações detalhadas de medidas de segurança, priorizadas conforme a criticidade dos riscos encontrados.

O IBLISS framework está sempre alinhado ao objetivos e negócio da Organização, baseado nas melhores práticas, normas e frameworks de mercado, analisando Tecnologias, Pessoas e Processos, permitindo identificar o nível de maturidade de Segurança da Informação e consolidando o resultado dentro da solução GAT, como demonstra na imagem abaixo.



HACKER AS A SERVICE

COMPONENTES DA OFERTA

IBLISS DIGITAL SECURITY

1. Análise técnica

2. Relatório de Riscos

3. Suporte a correção e validação

PTES Technical Guidelines

OWASP Open Web Application Security Project

NIST

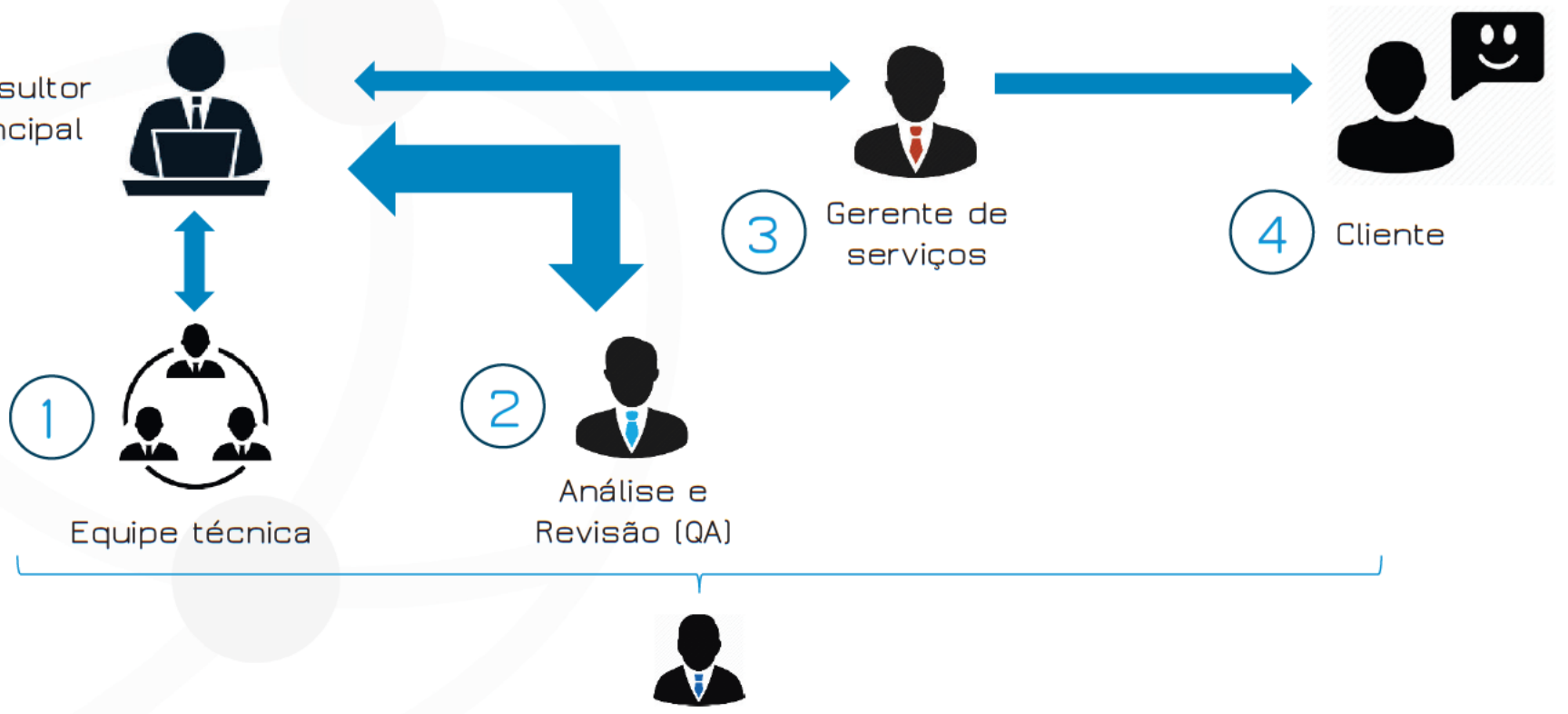
OSSTMM www.osstmm.org

ISSAF Information Systems Security Assessment Framework www.oissg.org

HACKER AS A SERVICE

PROCESSO DE EXECUÇÃO DO PROJETO

IBLISS DIGITAL SECURITY



HACKER AS A SERVICE

TIPOS DE TESTES

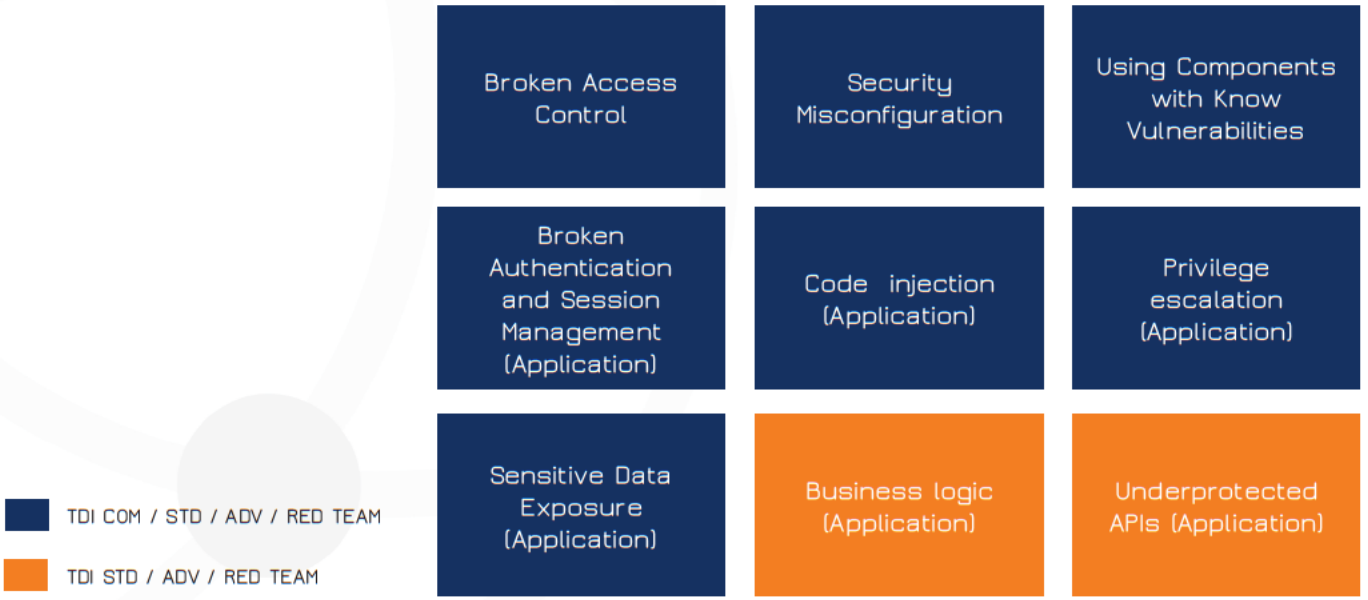
IBLISS DIGITAL SECURITY

	Teste de Invasão Compliance	Análise de Vulnerabilidades	Teste de Invasão Advanced	Red Team
Objetivo	Testes de segurança em todos os alvos do escopo	Testes de segurança em todos os alvos do escopo	Testes de segurança orientado aos objetivos específicos	Testes de segurança orientado aos objetivos específicos
Execução	Remoto/Local	Remoto/Local	Remoto	Remoto/Local
Scan de vulnerabilidades	√	√	√	√ (se necessário)
Validações de falsos positivos e consolidação de vulnerabilidades	√	√	√	√
Análises manuais*	√		√	√
Exploração da vulnerabilidade e movimentação lateral			√	√
Engenharia social (Phishing, Vishing, SMiShing)				√
Engenharia social (Físico)				√
OSINT - Open Source Intelligence			√	√
Wireless				√

HAAS - MODALIDADES

OPCÕES PARA EXECUÇÃO DO TESTE

Análises manuais - para as modalidades que possuem análises manuais os seguintes testes se aplicam



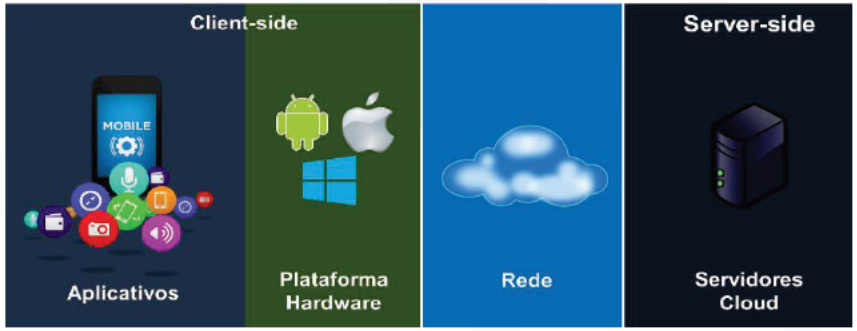
METODOLOGIA DE ANÁLISE

INFRAESTRUTURA / APP WEB

- Broken Access Control
- Information Gathering:
- Network Discovery / Network enumeration
- Network Port and Service Identification
- Password Cracking
- Privilege escalation
- Security Misconfiguration
- Sensitive Data Exposure
- Using Components with Known Vulnerabilities
- Vulnerability analysis / Scanning
- Broken Access Control (Authenticated users controls, Privilege escalation)
- Broken Authentication (Authentication and session management)
- Business logic
- Cross-Site Scripting (XSS)
- Data Validation Testing:
- Information Gathering:
- Insecure Deserialization
- Insufficient Logging&Monitoring
- Injection
- Underprotected APIs (Applications integration)
- Using Components with Known Vulnerabilities
- Web Services Testing:
- XML External Entities (XXE)

METODOLOGIA DE ANÁLISE

APP MOBILE



Análise de aplicação mobile

- Na análise de aplicativos mobile realizamos análise técnicas baseadas na seguinte metodologia

Client-side:

- Autenticação insegura
- Autorização insegura
- Armazenamento inseguro de dados
- Code tampering
- Criptografia insuficiente
- Engenharia reversa
- Funcionalidades externas, utilização de recursos externos a plataforma
- Uso de plataforma imprópria

Comunicação client-side e server-side

- Criptografia insuficiente
- Comunicação insegura

Server-side (Análise remota)

- Code injection
- Análise externa da infraestrutura

HAAS - MODALIDADES

OPCÕES PARA EXECUÇÃO DO TESTE

IBLISS DIGITAL SECURITY

	Acesso a Informações	Credenciais	URL/IP	Benefícios
White-Box	Sim	Sim	Sim	A partir das informações recebidas, pode ser feito um teste direcionado a aplicação, ao sistema operacional e dispositivos de rede. Obtendo melhores resultados na exploração das vulnerabilidades e falhas.
Grey-Box	Não	Sim	Sim	Para este teste é fornecido parcialmente informações sobre o ambiente analisado.
Black-Box	Não	Não	Não	O benefício deste teste é aplicar um ataque real, onde é pressuposto que um usuário mal intencionado não terá nenhuma informação sobre a aplicação.

HAAS - FERRAMENTAS

- Plataforma GAT - Para gestão de vulnerabilidades
- NMAP -Varredura de Portas;
- Maltego e Ferramenta própria - Levantamento de informações;
- Tenable Nessus Professional Feed - Levantamento de vulnerabilidades;
- W3AF - Levantamento de vulnerabilidades;
- Metasploit Framework e Exploit Tree - Exploração de vulnerabilidades;
- Acunetix - Avaliação das aplicações Web;
- Burp Professional Edtion - Avaliação das aplicações Web;
- SQL Map - Avaliação de Aplicações e Banco de Dados;
- Ferramentas OWASP - Avaliação das aplicações Web;
- Mobile Security Framework - Avaliação das aplicações Mobile;
- Entre outras ferramentas desenvolvidas internamente, sendo algumas publicada em:
  - https://github.com/iBLISSLabs1

ESCOPO DO PROJETO

O escopo para este projeto foi definido nos seguintes parâmetros:

- **Periodicidade:** Pontual
- **Tipo de teste:** Teste de invasão Advanced Black box em plataforma de voto eletrônico

Pentest

Aplicação WEB em BLACK-BOX – Plataforma de voto eletrônico conforme documento de especificação técnica

- **Reteste e suporte IBLISS para correções:** 60 dias após a entrega dos resultados
- **Acesso a plataforma GAT** durante 60 dias após a entrega dos resultados

EXECUÇÃO

- Todas as atividades e serviços serão executadas em horário comercial.
- O cliente deverá informar previamente os pontos de contatos principais e secundários para o acompanhamento desse contrato.
- Toda solicitação de um novo serviço deverá ser realizada ao Gerente Comercial da IBLISS responsável pelo acompanhamento do contrato.
- As equipes do Cliente e IBLISS deverão alinhar previamente qual o escopo necessário para cada atividade.
- O Cliente deverá informar a IBLISS qual o objetivo para cada atividade solicitada.
- A IBLISS informará ao Cliente qual o esforço necessário com relação a tempo e recursos disponíveis para a execução de cada atividade.
- O Cliente deverá aprovar previamente a realização das atividades considerando a quantidade de horas definidas pela IBLISS.
- Haverá gerenciamento constante das atividades, com objetivo de manter as partes informadas, resolver dificuldades e definir a necessidade de maior número de horas.
- Sempre que julgar necessário a IBLISS atuará de forma consultiva informando ao Cliente quais são as melhores práticas há serem estabelecidas para cada atividade.
- Vulnerabilidades detectadas:
    - Caso detectadas vulnerabilidades críticas, estas serão reportadas imediatamente por meio de relatórios emergenciais;
    - Caso seja identificada alguma vulnerabilidade que possa ocasionar a negação de serviço (DoS), a qual não faz parte do escopo, esta será informada ao responsável do cliente para que então seja tomada a decisão apropriada sobre a execução do teste.

CRONOGRAMA

De acordo com o escopo definido para o projeto, as atividades estão agrupadas em um cronograma que dará a adequada percepção e visão das fases, marcos de controle e esforço estimado para sua execução, a fim de permitir o acompanhamento do projeto.

Os trabalhos poderão ser iniciados em até 10 dias para serviços remotos e 30 dias para serviços in-loco a partir da assinatura deste contrato, mediante verificação de disponibilidade de equipe.

O cliente poderá utilizar o serviço contratado em até 6 meses após a assinatura do contrato, após esse prazo as condições do contrato podem ser revistas.

SUPORTE A CORREÇÃO DE VULNERABILIDADES E RETESTE

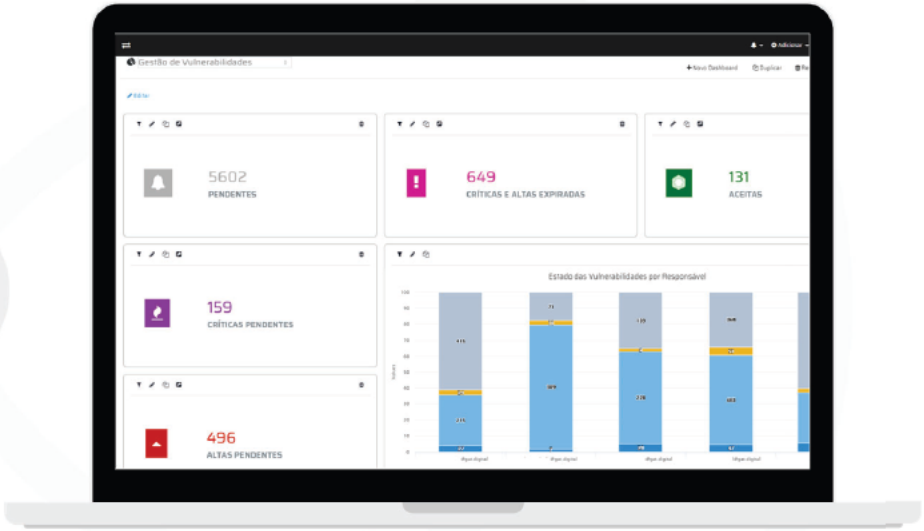
Após a geração dos relatórios finais e apresentação dos mesmos, é oferecido suporte às equipes técnicas para implementação das correções. Este apoio poderá ser utilizado durante 120 dias após a entrega dos testes.

O cliente também poderá solicitar em até 60 dias após a entrega do projeto o reteste para validação da correção das vulnerabilidades encontradas.

O suporte à correção será oferecido por nossa plataforma de suporte, por meio do e-mail suporte@ibliss.com.br

GAT - PLATAFORMA

IBLISS DIGITAL SECURITY



94%

Aumento do nível de Segurança Digital

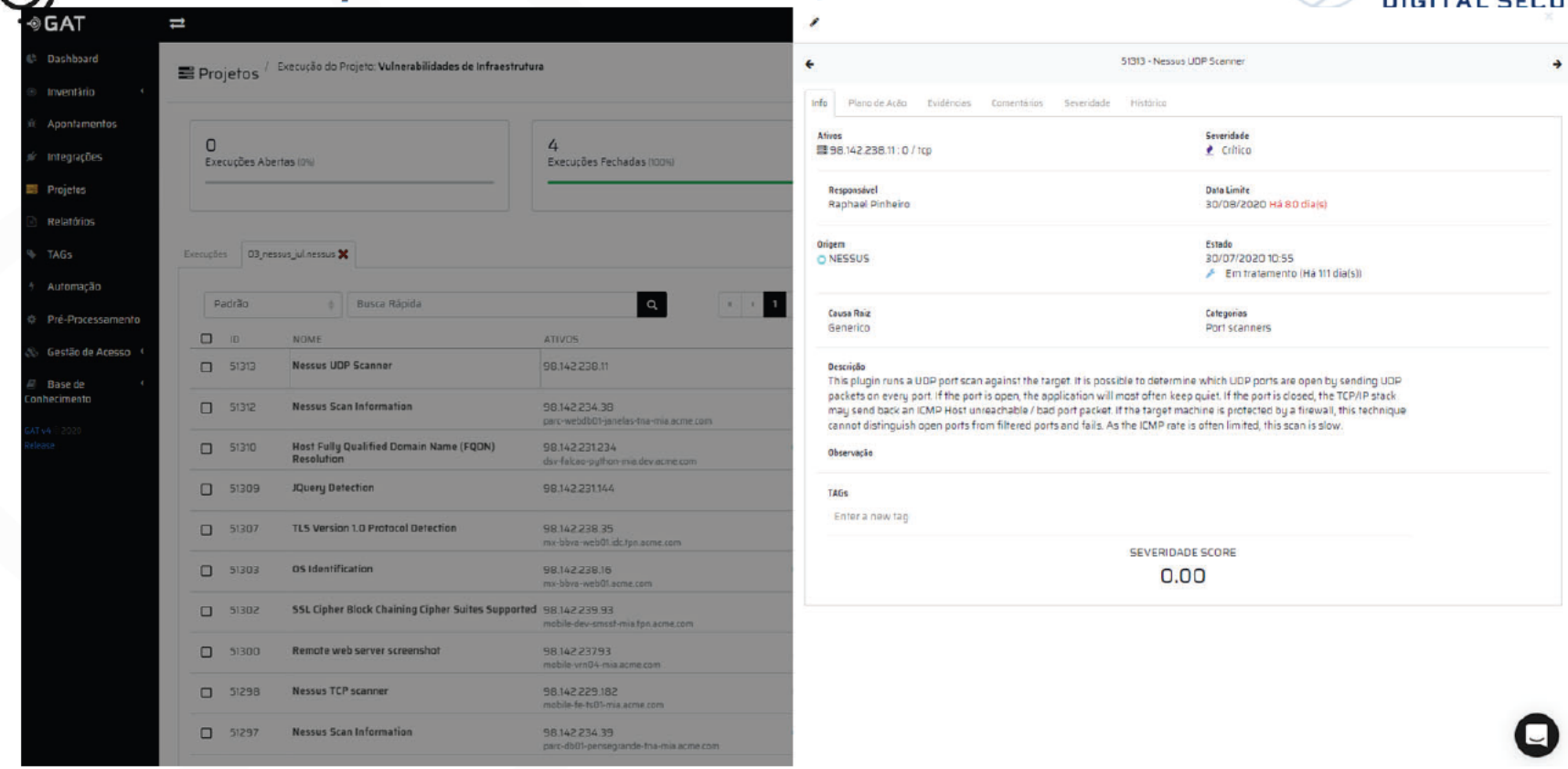
55%

Aumento da produtividade de analistas de TI / SI

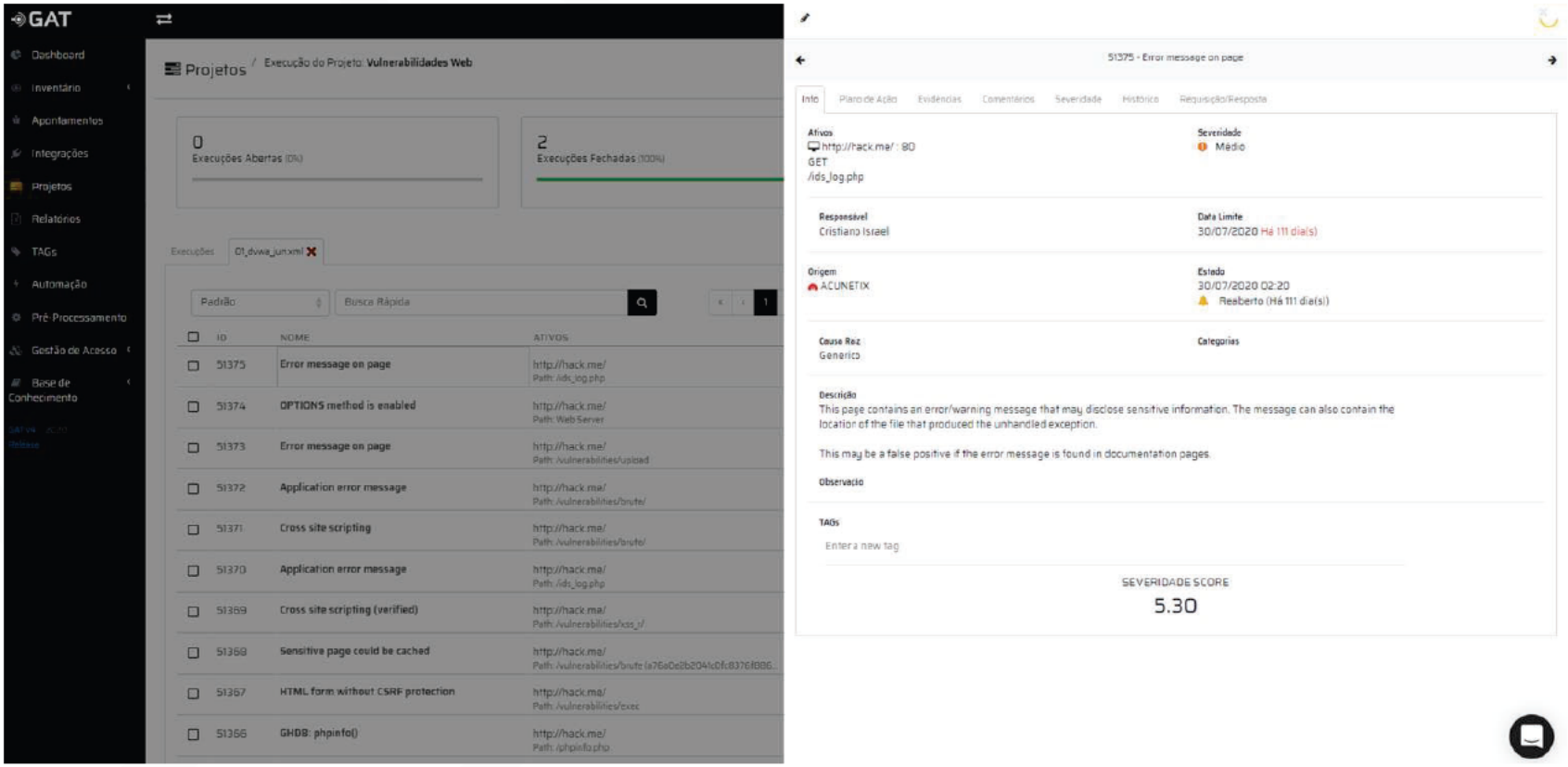
O: resultados serão disponibilizados na plataforma GAT pelo período de 60 dias, para até 02 usuários. Essa plataforma facilita o processo de correção dos pontos encontrados durante os testes, além de facilitar o compartilhamento dos resultados dos testes com as equipes responsáveis pelos ativos. As principais características são:

- Acompanhamento das correções;
- Fácil identificação dos ambientes mais críticos;
- Obtenção de maiores informações sobre cada vulnerabilidade;

ESTABELEÇA E MENSURE KPI's, KRI's e SLA's

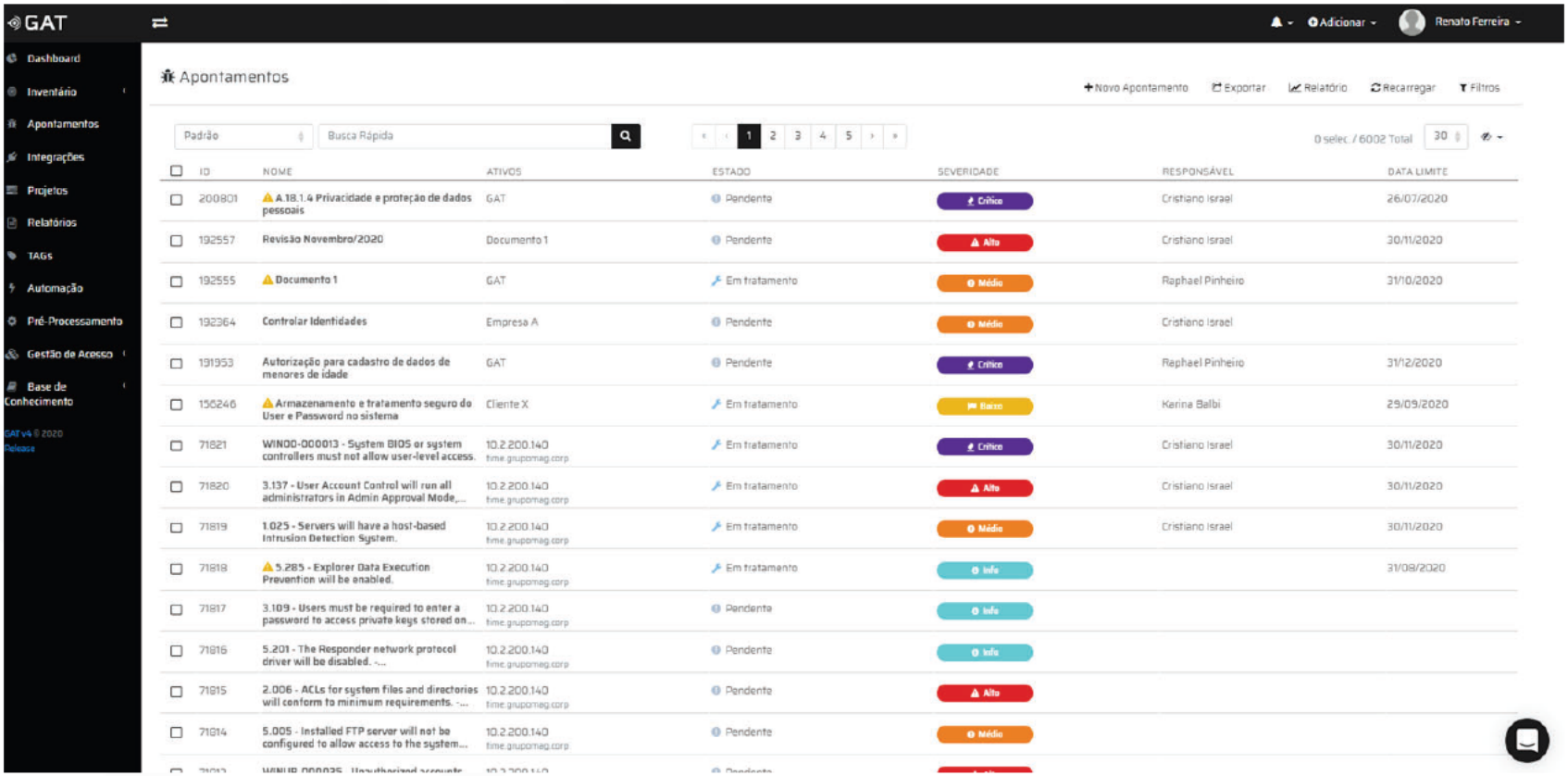


ESTABELEÇA E MENSURE KPI's, KRI's e SLA's



ESTABELEÇA E MENSURE KPI's, KRI's e SLA's

IBLISS DIGITAL SECURITY



Apontamentos

LIMITAÇÕES E RESPONSABILIDADES

Estão fora do escopo do projeto

- Realização de testes que tenham por objetivo causar indisponibilidade de serviços ou ativos de forma externa (DDoS, DoS, flood, etc);
- Análise local dos equipamentos, como, por exemplo, levantar e analisar as regras de firewall ou validar o uso de procedimentos de hardening nos servidores ou serviços;
- Avaliação de controles disponíveis somente do lado do servidor, bem como validação de regras de negócio;
- Execução da correção e implantação de soluções.
- URL´s e sistemas que não estejam dentro do especificado nessa proposta e de acordo com acordado no projeto.

Limitação

- A Contratante deve estar ciente de que serão tomadas todas as providências para que o teste não provoque indisponibilidade ou impacto na aplicação. No entanto, mesmo com os maiores cuidados aplicados, poderá haver algum comportamento não previsto, podendo afetar a estabilidade da aplicação. Como as condições de segurança dos equipamentos e aplicações são desconhecidas, reações inesperadas podem acontecer, dessa forma recomenda-se a definição de um ponto de contato de um técnico de suporte do cliente, mas a IBLISS irá apoiar todo processo até o restabelecimento do mesmo.

RECURSOS ALOCADOS

Sugerimos a constituição da seguinte equipe de projeto:

Do lado da IBLISS:

- 1 consultor sênior, que executará os trabalhos definidos nesta proposta;
- Equipe de pentesters que dão apoio técnico ao consultor principal;
- 1 gerente de projeto, que assegurará a boa execução dos trabalhos reportados nesta proposta, assim como servirá de ponto de contato privilegiado entre a equipe e o cliente;
- 1 gerente de QA, que irá revisar todas as entregas deste projeto.

Do lado do cliente:

- 1 responsável pelo acompanhamento da execução dos trabalhos do projeto e que servirá de ponto de contato.

CONDIÇÕES COMERCIAIS

Item	Atividades	Tempo execução	Valor R$
Hacker as a Service (HaaS)	Teste de invasão Advanced Black –Box Aplicação WEB	40 horas	R$12.000,00

- Valores expressos em Reais (R$) com base em Julho de 2021 e válidos por 30 (trinta) dias a contar da emissão desta proposta;
- O pagamento deverá ser realizado em parcela única 30 dias após a emissão da nota fiscal após o aceite
- Custos de deslocamento não estão inclusos no valor da proposta;
- Tributos já inclusos no valor apresentado.



IBLISS
DIGITAL SECURITY

Fernanda Olivato

Sales Account Manager

Fernanda.olivato@ibliss.com.br
+ 55 11 96300-7203
+ 55 11 3255-3926

Ibliss.com.br
Avenida Angélica, 2582 - Cj. 22
Higienópolis - São Paulo - Brasil

#porumasociedademaissegura

PROPOSTA
TÉCNICA COMERCIAL

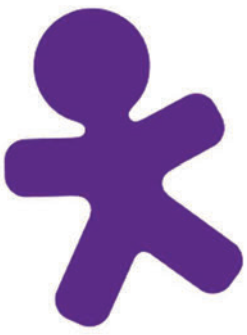
MINISTÉRIO PUBLICO DA BAHIA

Título: Pentest de Aplicação

Data: 20/07/2021

SFA: 1949964

Versão: 1.0



Sumário

1. VIVO 2
1.1. Institucional 2
1.2. Certificações 2
2. Segurança da Informação 3
2.1 Protegendo a informação 3
2.2 Ameaças Avançadas 4
3. Características do Produto 5
3.1 Metodologia 5
3.2 Enumeração de Vulnerabilidades 6
4. PORTFÓLIO DE EQUIPAMENTOS DE TI E PRESTAÇÃO DE SERVIÇOS 7
4.1 Prestação de Serviços 7
4.2 Teste de Invasão: 8
4.3 Características do Teste 9
4.4 Entregáveis 10
4.5 Limitações 10
5. Condições Gerais de Fornecimento 11
5.1 Responsabilidades Vivo Empresas 12
5.2 Responsabilidades da CONTRATANTE 12
5.3 Premissas 12
5.4 Condições Comerciais Equipamentos TI e Prestação de Serviço 14
5.4.1 Produtos de Revenda 14
5.4.2 Faturamento 14
6. VALIDADE DA PROPOSTA 14
7. CONFIDENCIALIDADE 14
8. ORIENTAÇÕES DIVERSAS 15

Propriedade da Telefônica. Toda e qualquer reprodução, distribuição, comunicação pública é expressamente proibida sem a sua prévia autorização.

SFA769866

Anexo Orcamento 03 (0164289) SEI 19.09.02684.0011790/2021-22 / pg. 144

1. VIVO

1.1. Institucional

A Vivo é a marca comercial da Telefônica Brasil, empresa líder em telecomunicações no País, com 97,8 milhões de acessos (1T18). A operadora atua na prestação de serviços de telecomunicações fixa e móvel em todo o território nacional e conta com um portfólio de produtos completo e convergente para clientes B2C e B2B – banda larga fixa e móvel, ultra banda larga (over fiber), voz fixa e móvel e TV por assinatura. A empresa está presente em 4,3 mil cidades, sendo 4,1 mil com rede 3G e mais de 2,7 mil com 4G, segmento em que é líder de Market Share. A operadora ainda oferece o 4G+, internet duas vezes mais rápida que o 4G. No segmento móvel, a Vivo tem 75,1 milhões de clientes e responde pela maior participação de mercado do segmento (31,9%) no país, de acordo com resultados do balanço trimestral (1T18).

Guiada pela constante inovação e a alta qualidade dos seus serviços, a Vivo está no centro de uma transformação Digital, que amplia a autonomia, a personalização e as escolhas em tempo real dos seus clientes, colocando-os no comando de sua vida digital, com segurança e confiabilidade. A Telefônica Brasil faz parte do Grupo Telefónica, um dos maiores conglomerados de comunicação do mundo, com presença em 21 países, 356,9 milhões de acessos, 122,8 mil colaboradores e receita de 52,0 bilhões de euros em 2017.

Ciente de sua responsabilidade de retribuir à sociedade a confiança que recebe na utilização dos seus serviços, a empresa conta com a Fundação Telefônica Vivo. Desde 1999, a Fundação atua na formação da nova geração, apontando os caminhos para o desenvolvimento do país ao aplicar inovação à educação, empreendedorismo e cidadania, com diferentes projetos sociais nessas áreas.

1.2. Certificações

A **Vivo** utiliza um conjunto de metodologias e melhores práticas reconhecidas pelo mercado para a prestação dos seus serviços.

A empresa tem como política e diretriz empresarial realizar forte investimento em processos e certificações para o aprimoramento da capacitação de seus profissionais e processos internos, melhoria da eficiência e, consequentemente, o aumento da qualidade dos serviços prestados. A **Vivo** entende que o sucesso na implementação dos processos de negócios está baseado em três dimensões: **Atitude**, **Tecnologia** e **Metodologia**.

Propriedade da Telefônica. Toda e qualquer reprodução, distribuição, comunicação pública é expressamente proibida sem a sua prévia autorização.
SFA769866

2. Segurança da Informação

2.1 Protegendo a informação

A informação é a alma da empresa moderna. É o seu ativo mais importante e atua como o fator-chave potencializador da atual economia baseada no conhecimento, uma vez que grande parte das atividades diárias dos funcionários requer a criação e o processamento de informação. Assim, proteger os ativos de informação tornou-se uma função-chave para as empresas.

Os serviços de Tecnologia de Informação e Comunicação (TIC) fornecem a infraestrutura necessária para os processos de negócios que permeiam a organização. Em um ambiente altamente competitivo, é fundamental processar a informação de forma eficaz e eficiente, possibilitando protegê-la contra a manipulação não autorizada ou simplesmente inadequada e divulgando-a somente aos recursos-chave que precisam ter acesso a esse conhecimento para realizar as suas tarefas. Ao mesmo tempo, deve-se mantê-la segura e protegida dos olhos curiosos das pessoas que não têm necessidade de acessar essas informações. Este paradigma estabelece um conjunto crescente de exigências de forma a apoiar eficazmente as necessidades dos novos negócios para a acessibilidade de informação que, muitas vezes, extrapola os limites físicos das instalações da empresa. Essa tendência é agravada pela nossa própria necessidade de conectar-nos com os nossos clientes e parceiros de negócios, compartilhar informações e proporcionar novos canais de comunicação.

Ao mesmo tempo, as empresas estão sujeitas a um cenário de ameaças cada vez mais complexo, bem como a pressões reguladoras e padrões industriais de conformidade que requerem um grande nível de especialização e um aumento dos níveis de investimento de capital. Esta tendência não mostra sinais de redução.

Hoje os ataques são direcionados e têm uma motivação financeira. Os tempos em que os malwares eram criados por curiosidade ou para ganhar visibilidade, como uma forma de ganhar fama, já passaram. A maioria destes malwares, também conhecidos como “vírus tradicionais", causavam um grande impacto sobre os recursos de processamento de informações da empresa e podiam ser facilmente descobertos. Hoje, os números são surpreendentes:

- 50 mil novos malwares são detectadas diariamente por empresas de pesquisa de segurança;
- Mais de 200 mil novos sites maliciosos são criados mensalmente.

Os clientes exigem, portanto, que prestadores de serviço reduzam a complexidade inerente a estas realidades, fornecendo soluções e serviços de segurança de custo eficaz que lhes permita concentrar no seu objetivo principal de negócio.

Propriedade da Telefônica. Toda e qualquer reprodução, distribuição, comunicação pública é expressamente proibida sem a sua prévia autorização.
SFA769866

Anexo Orcamento 03 (0164289) SEI 19.09.02684.0011790/2021-22 / pg. 146

2.2 Ameaças Avançadas

Como os ataques estão se tornando cada vez mais sofisticados, o malware foi substituído por outros vetores de ataque. Alguns exemplos dessas novas ameaças incluem:

Botnets	Grupos de computadores infectados controlados remotamente por atacantes maliciosos com objetivo de serem utilizados para coletar informações pessoais, cometer fraudes e roubo de identidade, realizar ataques em massa de negação de serviço em sites e empresas, ou enviar grandes quantidades de e-mail não solicitadas (spam).
Sites legítimos infectados	Os atacantes controlam de forma regular sites de renome usando-os para disseminar malwares clandestinamente para usuários desavisados da web, através de, por exemplo, código malicioso injetado dentro de sites legítimos.
Cross-site scripting (ataques XSS)	Links para sites maliciosos incorporados dentro de outro tipo de conteúdo legítimo para que o usuário web, que acesse um site legítimo, também faça o download do código malicioso hospedado em sites externos ilícitos de maneira automática, sem intervenção ou conhecimento do usuário.
Otimização dos Motores de busca maliciosos (SEO)	A maioria dos usuários conta com motores de busca como Google ou Bing como motores de busca. Os atacantes usam este comportamento contra esses usuários, abusando dos algoritmos que estes motores usam para classificar os resultados. Quando uma notícia de grande repercussão é divulgada, os atacantes produzem rapidamente sites maliciosos sobre tal acontecimento, que promovidos para itens mais bem classificados nos resultados da pesquisa, ficam mais propensos a serem visitados por usuários desavisados que querem saber mais sobre o ocorrido.
Antivírus Falso	Um site malicioso produz um alarme que, para o usuário web, parece um alarme legítimo emitido por um motor antivírus. Este alarme informa o usuário que a sua máquina foi comprometida e que é necessário instalar um antivírus. Quando o usuário concorda, o malware é descarregado para a máquina que passa, então, a ser controlada, tornando-se parte de uma botnet.

Com o tempo, tornam-se cada vez mais comuns este tipo de ameaças sofisticadas. Uma estratégia de proteção eficaz requer mecanismos de adaptação e evolução frente às novas ameaças, mostrando-se como um grande desafio às organizações.

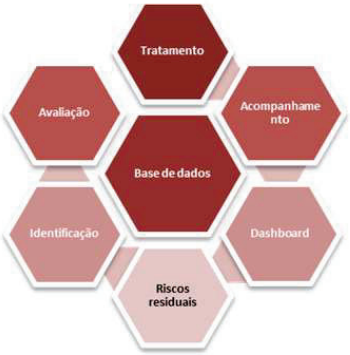
Propriedade da Telefônica. Toda e qualquer reprodução, distribuição, comunicação pública é expressamente proibida sem a sua prévia autorização.
SFA769866

Anexo Orcamento 03 (0164289) SEI 19.09.02684.0011790/2021-22 / pg. 147

3. Características do Produto

3.1 Metodologia

De acordo com o nível de informações que serão passadas sobre o ambiente, o teste pode ser classificado como Black Box (caixa preta), White Box (caixa branca) ou Grey Box (caixa cinza) (híbrido).



Em um teste Black Box, há pouco ou nenhum conhecimento sobre o ambiente a ser avaliado, e tudo deve ser descoberto pelo analista.

Em testes White Box, analogamente, o avaliador tem acesso irrestrito a qualquer informação que possa ser relevante ao teste, para conduzi-lo supondo o pior cenário, em que o atacante conseguiu obter todos os detalhes sobre o(s) alvo(s).

Dentro do contexto da metodologia de execução de projetos Vivo Empresas, os Testes de Invasão deverão ter escopo bem definido, visando minimizar o potencial de erros durante o processo de simulação de ataque. Também deverão ser formalmente autorizados antes de sua execução, garantindo assim a conformidade legal do projeto.

Este trabalho de consultoria tem entre os seus objetivos fornecer orientações estruturadas sobre ações preventivas e corretivas, contribuindo assim para o processo de gestão de Riscos Corporativos e de Segurança da Informação, conforme orientações das normas ABNT/NBR ISO/IEC 27005 e ISO 31000. Sendo assim, nos produtos finais (entregáveis) conterão descrições das vulnerabilidades encontradas, bem como o correspondente grau de risco no contexto onde foram encontradas, bem como orientações sobre procedimentos que poderão ser adotados para corrigir as possíveis falhas encontradas.

Abaixo descrevemos exemplos de relatórios que farão parte dos produtos finais:


Teste de Invasão | TESB

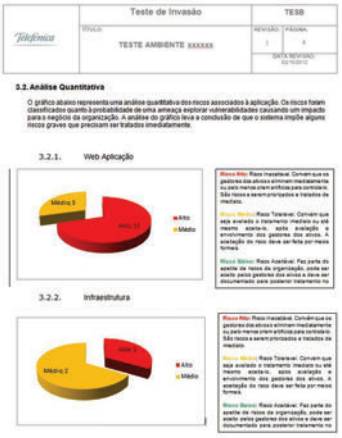
TESTE AMBIENTE xxxxxx

3.1. Riscos

A tabela abaixo demonstra as vulnerabilidades encontradas e os critérios de Impacto e Probabilidade que compõem o Risco de cada vulnerabilidade.

3.1.1. Web Aplicação

ID	Vulnerabilidade	Impacto	Probabilidade	Risco
Alvo: www.111111.com.br				
6.1.1.1.1	Acesso Indevido	Alto	Alto	Alto
6.1.1.1.2	Acesso Indevido	Alto	Alto	Alto
6.1.1.1.3	Injeção de Código Malicioso	Alto	Alto	Alto
6.1.1.1.4	Injeção de Código Malicioso	Alto	Alto	Alto
6.1.1.1.5	Dados do Servidor Exposto	Alto	Alto	Alto
6.1.1.2.1	Informações Expostas	Médio	Médio	Médio
6.1.1.2.2	Métodos de Acesso Habilitados	Baixo	Alto	Médio
Alvo: www.222222.com.br				
6.1.2.1.1	Injeção de Código Malicioso	Alto	Alto	Alto
6.1.2.1.2	Acesso Indevido	Alto	Alto	Alto
6.1.2.1.3	Versão Exposta	Alto	Alto	Alto
6.1.2.2.1	Informações Expostas	Médio	Médio	Médio
6.1.2.2.2	Métodos de Acesso Habilitados	Baixo	Alto	Médio
Alvo: www.333333.com.br				
6.1.3.1.1	Acesso Indevido	Alto	Alto	Alto
6.1.3.1.2	Dados do Servidor Exposto	Alto	Alto	Alto
6.1.3.1.3	Informações Expostas	Alto	Alto	Alto
6.1.3.1.4	Injeção de Código Malicioso	Alto	Alto	Alto
6.1.3.2.1	Métodos de Acesso Habilitados	Baixo	Alto	Médio


Teste de Invasão | TESB

TESTE AMBIENTE xxxxxx

3.2. Análise Quantitativa

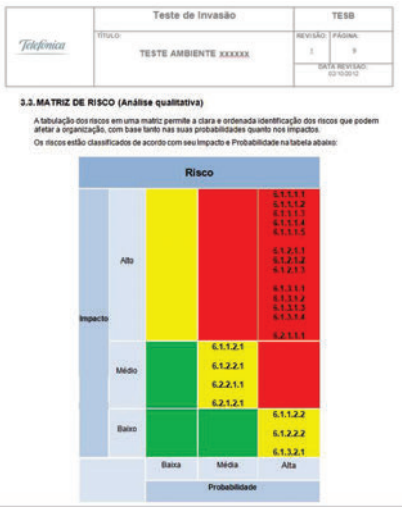
O gráfico abaixo representa uma análise quantitativa dos riscos associados à aplicação. Os riscos foram classificados quanto à probabilidade de uma ameaça explorar vulnerabilidades causando um impacto para o negócio da organização. A análise do gráfico leva a conclusão de que o sistema impõe alguns riscos graves que precisam ser tratados imediatamente.

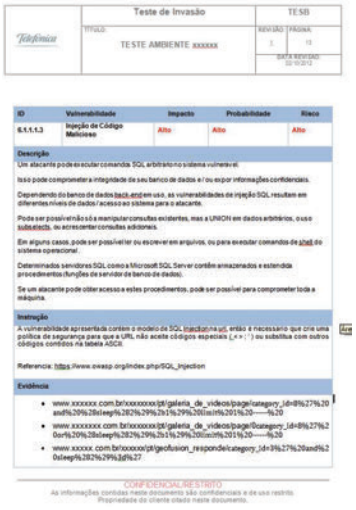
3.2.1. Web Aplicação

3.2.2. Infraestrutura

Propriedade da Telefônica. Toda e qualquer reprodução, distribuição, comunicação pública é expressamente proibida sem a sua prévia autorização.
SFA769866

Anexo Orcamento 03 (0164289) SEI 19.09.02684.0011790/2021-22 / pg. 148





Embora o processo de execução das simulações de ataque ocorra com base na experiência de profissionais especializados neste tipo de trabalho, algumas ferramentas são utilizadas para melhor enumeração de vulnerabilidades e avaliações dos riscos associados.

3.2 Enumeração de Vulnerabilidades

Análise de Aplicações Web:

- Injeção de Código Malicioso;
- Cross-site Script (XSS – CSRF);
- Sql Injection;
- Atualização de Sistema (Hardening);
- Enumeração de Diretório;
- Acesso Indevido (Bypass).

Análise de Infraestrutura:

- Atualização do Ambiente (Hardening);
- Acesso Indevido (Bypass);
- Sistemas Habilitados Desnecessários;
- Sistemas Habilitados com versão vulnerável possibilitando Acesso;
- Ataque de Força Bruta (Brute Force).

Propriedade da Telefônica. Toda e qualquer reprodução, distribuição, comunicação pública é expressamente proibida sem a sua prévia autorização.
SFA769866

4. PORTFÓLIO DE EQUIPAMENTOS DE TI E PRESTAÇÃO DE SERVIÇOS

4.1 Prestação de Serviços

Realização de PENTEST de Aplicação Web:

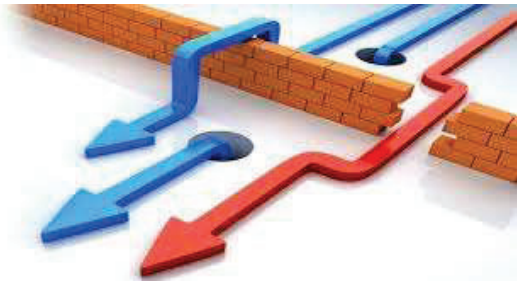
Cliente	Ministério Público da Bahia
Pentest:	Blackbox
Escopo:	Aplicação Web
Estimativa:	30 dias

Blackbox - Ataque externo

A aplicação a ser testada chama-se APLICAÇÃO X, hospedada em 1 servidor web de pequeno porte. Os testes de blackbox externos consistem em simular um cenário de ataque, como qualquer pessoa conectada à Internet, para identificar as violações de segurança existentes no ambiente target que podem colocar em risco as informações processadas e / ou armazenadas lá, ou que pode servir de base para atacar outros ativos tecnológicos do MINISTERIO PUBLICO DA BAHIA.

Propriedade da Telefônica. Toda e qualquer reprodução, distribuição, comunicação pública é expressamente proibida sem a sua prévia autorização.
SFA769866

4.2 Teste de Invasão:



A realização dos testes propostos seguirá as seguintes características:

- Os testes podem ser acompanhados por um responsável da CONTRATANTE;
- O Período de testes, TDI, Coleta de Dados e documentação seguirá conforme Termo de Referência;
- A metodologia utilizada será Blackbox, conforme item 4.1;
- As vulnerabilidades identificadas serão notificadas por meio de relatório técnico, incluindo suas respectivas classificações de risco;
- Serão documentadas e apresentadas as recomendações necessárias para correção dos pontos de vulnerabilidade identificados;
- Entregar e apresentar relatório executivo sobre as vulnerabilidades encontradas.

Propriedade da Telefônica. Toda e qualquer reprodução, distribuição, comunicação pública é expressamente proibida sem a sua prévia autorização.
SFA769866

Anexo Orcamento 03 (0164289) SEI 19.09.02684.0011790/2021-22 / pg. 151

4.3 Características do Teste

Abaixo apresentamos uma visão por fases, para a execução das tarefas planejadas para este projeto, bem como os entregáveis previstos para cada fase:

FASE 01 – PLANEJAMENTO DO PROJETO, ESTABELECIMENTO DE METODOLOGIA E CRITÉRIOS.

Esta fase é obrigatória em todos os projetos de Consultoria em Segurança da Informação da Vivo Empresas, de acordo com a Metodologia de Execução de Projetos. Nesta oportunidade, serão detalhadas todas as atividades, os recursos necessários para sua execução, os prazos estimados para cada atividade e os produtos que deverão ser gerados em cada fase. O cliente deve aprovar o planejamento do projeto, antes que os trabalhos tenham início.

Nesta fase geramos os primeiros Entregáveis do Projeto, que é composto de:

- Relatório de Especificação do Planejamento do Projeto;
- Cronograma detalhado do Projeto;
- Apresentação do Planejamento do Projeto para patrocinadores e outas pessoas envolvidas;

FASE 02 – ANÁLISE DE VULNERABILIDADES DE SEGURANÇA DE REDE E APLICAÇÕES WEB:

Nesta fase, iniciamos as atividades de Pentest em Aplicação Web. Em síntese, esta fase se subdividirá em:

- Análise de Vulnerabilidades de Segurança: Mapeamento de vulnerabilidades e falhas de segurança, em aplicações web e/ou configurações da infraestrutura que suportam o ambiente;
- Apontamento de Recomendações e/ou Oportunidades de Melhorias para a correção destas vulnerabilidades ou mitigação do risco através da implementação de controles de segurança.
- Cobertura das Análises: Os testes contemplarão, no mínimo, 66 testes que estão detalhados no OWASP Testing Guide v4.0. Tais testes serão realizados de maneira automatizada e manual, conforme metodologia definida pela Vivo Empresas para a execução deste projeto.
- Reuniões Intermediárias de apresentação de resultados parciais;
- Apresentação dos Produtos Finais – Resultados dos Testes e Recomendações para cada Vulnerabilidade Encontrada.
- Contempla a realização de Testes de Invasão nos ambientes informados pela CONTRATANTE por Consultor Sênior/Especialista.

Propriedade da Telefônica. Toda e qualquer reprodução, distribuição, comunicação pública é expressamente proibida sem a sua prévia autorização.

SOBRE A EXECUÇÃO DO PROJETO

Deverá ser definida junto a CONTRATANTE a estratégia que será utilizada identificando e definindo os itens que irão compor as atividades do projeto;

Esta proposta não considera a utilização de técnicas que possam causar a indisponibilidade do ambiente, tais como: DDoS, tentativa de exploração automatizada de vulnerabilidades, brute force (em relação à técnica brute force, serão testadas senhas em branco e default);

4.4 Entregáveis

O relatório será entregue por meio seguro, contendo o resultado da avaliação realizada nos ambientes e as vulnerabilidades identificadas durante o teste. Faz parte do relatório apresentar os seguintes conteúdos:

• Sumário Executivo – apresentação de forma resumida do status dos trabalhos e o grau de exposição do ambiente às ameaças de mercado. Este relatório conterá um histórico com a evolução da situação real do ambiente diante das vulnerabilidades, as conclusões do trabalho, bem como as recomendações referentes às vulnerabilidades.

• Descritivo Técnico – será apresentado o resultado da avaliação realizada nos ambientes tecnológicos e as eventuais fragilidades identificadas durante o Teste. O relatório abordará recomendações concretas para correção das vulnerabilidades encontradas. Também será apresentada a priorização para cada vulnerabilidade diagnosticada de acordo com o seu respectivo grau de risco;

4.5 Limitações

Não fazem parte do escopo do trabalho aqui proposto:

- Configuração e/ou manipulação de equipamentos, hardware de propriedades da CONTRATANTE, salvo em atividade de contratação, acordada e autorizada para a execução de PENTESTs;
- Desenvolvimento e correção de código de software, arquiteturas de bancos de dados como entregas de projeto, entre outros.
- Responsabilização para a Vivo Empresas em processo de seleção de empresas. A indicação de empresas prestadoras e fornecedores de solução é um serviço de consultoria com vistas facilitação e aconselhamento nos trabalhos a serem executados. A responsabilidade pelo

Propriedade da Telefônica. Toda e qualquer reprodução, distribuição, comunicação pública é expressamente proibida sem a sua prévia autorização.

Anexo Orcamento 03 (0164289) SEI 19.09.02684.0011790/2021-22 / pg. 153

processo de requerimento por proposta para empresas indicadas ou não, seleção e compra de solução ficam reservados, única e exclusivamente ao CONTRATANTE, seus profissionais e seus processos internos.

- Elaboração de Normas específicas de segurança da informação e/ou procedimentos de segurança de qualquer natureza não ligados ao ambiente da proposta;
- Correção de vulnerabilidades encontradas durante a realização dos trabalhos;
- Implementação ou manipulação de regras em firewall, IPS, IDS, roteadores, switches e/ou sistemas de informação e segurança de qualquer natureza;
- Análise de segurança lógica em outros sistemas de computadores e redes de comunicação não destacados no escopo;
- Análises de segurança de aplicações corporativas, suas especificações e suas funcionalidades fora do âmbito do escopo;
- Análise de segurança dos bancos de dados nos aspectos de modelagem e estruturação de seus databases de aplicação;
- Avaliação, fornecimento e implementação de ferramentas que eventualmente sejam recomendadas pela análise de vulnerabilidades, nem de outras ferramentas que venham a ser necessárias;
- Execução de atividades ligadas à Ethical Hacking (ETH) ou outros formatos e métodos de avaliação de vulnerabilidades tipo manual;
- Atendimento a demandas que envolvam trabalho fora do horário comercial. Se surgirem necessidades deste tipo, a Vivo Empresas deverá ser formalmente comunicada, a fim de que um plano de trabalho possa ser avaliado e aprovado pelas partes, atendendo assim a legislação trabalhista vigente.

5. Condições Gerais de Fornecimento

As partes concordam que as suas equipes profissionais lhes são necessárias para o desempenho das suas atividades e execução do projeto. Assim, durante a vigência do mesmo e até 1 (um) ano após o seu término, nenhuma das partes contratará direta ou indiretamente qualquer profissional que tenha mantido contrato com a outra parte nos 12 (doze) meses precedentes.

No caso de violação do aqui disposto, a parte infratora ficará obrigada a pagar à outra parte a importância equivalente ao total pago ao profissional indevidamente recrutado nos doze últimos meses de vínculo com a parte lesada.

Propriedade da Telefônica. Toda e qualquer reprodução, distribuição, comunicação pública é expressamente proibida sem a sua prévia autorização.
SFA769866

Anexo Orcamento 03 (0164289) SEI 19.09.02684.0011790/2021-22 / pg. 154

5.1 Responsabilidades Vivo Empresas

A Vivo Empresas se compromete a executar os serviços propostos observando rigorosamente as condições ajustadas em relação a padrões, prazos e produtos.

A Vivo Empresas e seus prepostos se comprometem a dar tratamento confidencial aos fatos e informações reservadas aos quais tiverem acesso no decorrer dos trabalhos. Após a aprovação da presente proposta a Vivo Empresas designará um gerente de projetos a fim de atuar como responsável pelos serviços junto ao CONTRATANTE.

5.2 Responsabilidades da CONTRATANTE

É responsabilidade da CONTRATANTE, designar os seus representantes na equipe do projeto, com a disponibilidade necessária para participar de todas as atividades previstas no plano de trabalho.

A CONTRATANTE deverá manter total confidencialidade em relação às técnicas, instrumentos e metodologias aplicados pela Vivo Empresas na prestação dos serviços objeto desta proposta.

Mudanças nos sistemas e ferramentas de TI, equipes internas e/ou nas atividades da CONTRATANTE que porventura venham a ocorrer serão objeto de negociação complementar entre as partes, sempre que estas mudanças demandarem carga horária complementar relacionadas com a revisão das atividades e da documentação já elaborados e apresentados à CONTRATANTE.

Muitos dos nomes de serviços e de empresas referidas neste documento são marcas registradas. Todas elas são reconhecidas mediante esta declaração.

Neste período, o planejamento de projeto deverá cobrir todos os gaps de requisitos nos quais a Vivo Empresas se predispõe e coloca à disposição os profissionais designados para atender o requerido no planejamento de projeto.

Atrasos provocados na contratação de fornecedores e soluções e/ou no fornecimento e/ou implementações, correções, etc, provocados por terceiros ou a própria CONTRATANTE não poderão onerar o tempo de contratação, ficando a Vivo Empresas isenta de responsabilização por tais atrasos.

5.3 Premissas

As seguintes premissas são consideradas para que a prestação dos serviços ocorra da forma esperada:

- Não será empregado qualquer técnica ou artifício que envolva engenharia social, como envio de mensagens de e-mail contendo phishing, mensagens do tipo SMS ou ligações telefonicas com ID reais ou forjadas para obteção de informações;

Propriedade da Telefônica. Toda e qualquer reprodução, distribuição, comunicação pública é expressamente proibida sem a sua prévia autorização.
SFA769866

Anexo Orcamento 03 (0164289) SEI 19.09.02684.0011790/2021-22 / pg. 155

- Nos cenários de testes de infraestrutura externa, todos os testes e tentativas serão realizados de forma remota;
- Não está previsto qualquer atuação interna de forma presencial ou remota através de VPN/dispositivos de acesso remoto;
- O início das atividades contratadas está condicionado com a realização de um kickoff entre as equipes da Vivo Empresas S/A e o cliente e com o preenchimento e assinatura do Termo de Autorização;
- Não está previsto a análise de qualquer aplicativo móvel relacionado a empresa, ao sistema ou URL a ser analisada;

Propriedade da Telefônica. Toda e qualquer reprodução, distribuição, comunicação pública é expressamente proibida sem a sua prévia autorização.
SFA769866

Anexo Orcamento 03 (0164289) SEI 19.09.02684.0011790/2021-22 / pg. 156

5.4 Condições Comerciais Equipamentos TI e Prestação de Serviço

5.4.1 Produtos de Revenda

Os preços dos serviços constantes nesta proposta estão expressos em Reais refletem os impostos, taxas, contribuições vigentes na época da confecção desta Proposta. Caso haja alguma alteração para mais ou para menos destas condições, incluído a supressão ou adição de novos impostos, taxas, a Vivo Empresas se reserva no direito de efetuar os devidos ajustes de preços correspondentes.

Item	Descrição do Serviço	Valor à Vista c/ impostos
01	Pentest de Aplicação (30 dias)	R$ 41.186,85

5.4.2 Faturamento

O faturamento/cobrança dos serviços será à vista com vencimento em 30 dias a partir da data de emissão da Nota Fiscal.

ESTEIRA DE FATURAMENTO

- Faturamento T-Bra - Telefônica Brasil S.A

6. VALIDADE DA PROPOSTA

Os preços apresentados nesta Proposta são válidos por 10 (dez) dias contados a partir da data de sua entrega, salvo alterações macro ou microeconômicas significativas na economia do país.

7. CONFIDENCIALIDADE

A Vivo está ciente que as informações contidas comerciais neste documento são confidenciais e não deverão ser divulgadas fora do âmbito desta. O cliente autoriza a Vivo utilizar suas informações, tanto cadastrais quanto de perfil de consumo de tráfego, para análises internas.

Desde já aceita e concorda que a Vivo poderá dar publicidade do presente Projeto, a qualquer tempo, em mídia impressa e eletrônica, no território brasileiro ou fora dele, exclusivamente para divulgação de case, sem que se caracterize uso indevido de marca, nome comercial, imagem e/ou de quaisquer direitos do Cliente.

Propriedade da Telefônica. Toda e qualquer reprodução, distribuição, comunicação pública é expressamente proibida sem a sua prévia autorização.
SFA769866

Anexo Orcamento 03 (0164289) SEI 19.09.02684.0011790/2021-22 / pg. 157

8. ORIENTAÇÕES DIVERSAS

Este documento é uma proposta comercial. A contratação do serviço ficará pendente da assinatura do contrato.

Só serão aceitas solicitações de serviços que forem devidamente acompanhadas do Contrato social e Procuração da pessoa que assinou o presente instrumento. Será necessário informar os Cartórios para reconhecimento de firma do Cliente.

IMPORTANTE: Es Sumário Executivo/Proposta Comercial, o Termo de Contratação/Formulário e seus anexos estão sujeitos a viabilidade técnica.

Propriedade da Telefônica. Toda e qualquer reprodução, distribuição, comunicação pública é expressamente proibida sem a sua prévia autorização.
SFA769866

Anexo Orcamento 03 (0164289) SEI 19.09.02684.0011790/2021-22 / pg. 158

São Paulo, 20 de julho de 2021

A/C MINISTERIO PUBLICO DA BAHIA,

A Vivo é uma empresa que conhece as necessidades específicas de seus clientes e oferece as soluções mais avançadas em telecomunicações e serviços digitais com o melhor custo-benefício.

Agradecemos a oportunidade de apresentar esta proposta para a prestação de nossos serviços adequando às necessidades da sua empresa.

Antecipadamente nos colocamos à sua disposição para esclarecer ou revisar quaisquer itens a seguir descritos, para que a nossa proposta esteja plenamente alinhada com as suas necessidades.

Atenciosamente,

Emília Pitanga Sampaio Mettig
Diretoria de Governo | Gerencia Governo FSP
Gerente de Negocios – Especialista Governo
Tel.: (071) 99980-2026
Rua Silveira Martins, nº1036, Módulo 6, Cabula,
Salvador (BA), Cep.:41150-000
emilia.mettig@telefonica.com

Cristiane Soares Nunes Couto
Gerente Negócios Serviços Digitais
Div. Serviços Digitais
Cel + 55 11 95665- 9246
Av. Engenheiro Luis Carlos Berrini, 1376 – 28° Andar
04571-000 | São Paulo – SP
cristiane.couto@telefonica.com

Lival Estrela
Consultor de Soluções e Negócios | Pré-Vendas Gov. Federal e Regionais | PWF#F02
Diretoria de Produtos, Pré-Vendas e Pós-Vendas | Telefônica Brasil
Rua Silveira Martins 1036, Módulo 6, 1 andar
CEP 41150-000 | Salvador - BA
Cel + 55 71 99980-2365
lival.estrela@telefonica.com

Propriedade da Telefônica. Toda e qualquer reprodução, distribuição, comunicação pública é expressamente proibida sem a sua prévia autorização.
SFA769866

MINISTÉRIO PÚBLICO
DO ESTADO DA BAHIA

MANIFESTAÇÃO

Á Execução Orçamentária - DTI

Cumprimetamos cordialmente, encaminhamos o processo SEI para as devidas informações orçamentárias, com posterior retorno a esta unidade CASI-DTI

Documento assinado eletronicamente por **Iaçanã Lima de Jesus Carneiro** em 28/07/2021, às 12:58, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.sistemas.mpba.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0165189** e o código CRC **F6E3D478**.

Formulário de Informações Orçamentárias

Projeto / Ação / Atividade (número e nome):
2002 - MANUTENÇÃO DE SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Código da Unidade Orçamentária:
40601

Código da Unidade Gestora:
0003

Saldo Orçamentário:
R$ 2.149.795,28

Natureza da Despesa:
33.90.40

Responsável pela Informação:
JORGE ALBERTO DOS SANTOS CONCEIÇÃO

Responsável pela Unidade Gestora:
YURI GONZALEZ ARAÚJO

Número Sequencial da Dispensa / Inexigibilidade (Unidade Gestora):
11790/2021

Documento assinado eletronicamente por **Jorge Alberto dos Santos Conceicao** em 28/07/2021, às 13:58, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.sistemas.mpba.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0165242** e o código CRC **765EEA89**.

MINISTÉRIO PÚBLICO
DO ESTADO DA BAHIA

MANIFESTAÇÃO

À CASI/DTI

Prezado Coordenador, boa tarde!

Cumrpimentando-o cordialmente, encaminho o **PROCESSO SEI Nº 11790/2021 - DISPENSA DE LICITAÇÃO,** com devidas Informações Orçamentárias, estando o Processo **APTO** para prosseguimento regular.

Atenciosamente.

Jorge Alberto dos santos Conceição

Assistente Técnico Administrativo

Diretoria de Tecnologia da Informação - DTI

Execução Orçamentária

Documento assinado eletronicamente por **Jorge Alberto dos Santos Conceicao** em 28/07/2021, às 14:02, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.sistemas.mpba.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0165245** e o código CRC **E3E76E3E**.

MINISTÉRIO PÚBLICO
DO ESTADO DA BAHIA

MANIFESTAÇÃO

À Diretoria/DTI

Prezado Diretor, boa tarde!

Cumrpimentando-o cordialmente, encaminho o **PROCESSO SEI Nº 11790/2021 - DISPENSA DE LICITAÇÃO,** já com as devidas Informações Orçamentárias. Conforme documento "Passo a passo - Dispensa de Licitação Geral - Versão Final -11-02-2021 - falta acrescentar a CI que tem que ser assinada pelo nosso *"superiior imediato"* conforme passos elencados abaixo, parte do referido documento:

Incluir a documentação exatamente nessa ordem para melhor visualização na árvore do processo e com a nomenclatura sugerida (em negrito e na cor azul).

o ***DOD – Nome do objeto.docx***

o Comunicação Interna.pdf (A CI poderá ser feita em Word e assinada eletronicamente pelo promotor/superior imediato)

o Orçamento 01.pdf (orçamento do fornecedor vencedor) o

Certidão FGTS.pdf

o Certidão Trabalhista.pdf

o Certidão Municipal.pdf

o Certidão Estadual.pdf

o Certidão Federal.pdf

o Cadastro Pessoa Jurídica.pdf(se Pessoa Jurídica)

o Alvará de funcionamento.pdf (se Pessoa Jurídica)

o Contrato Social.pdf(se Pessoa Jurídica)

o RG.pdf (documento de identificação pessoal que tenha CPF)

o Comprovante bancário.pdf (em nome da empresa, se pessoa jurídica)

o Orçamento 02.pdf

o Orçamento 03.pdf

Atenciosamente.

Documento assinado eletronicamente por **Iaçanã Lima de Jesus Carneiro** em 28/07/2021, às 14:47, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.sistemas.mpba.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0165287** e o código CRC **87D67E34**.

MINISTÉRIO PÚBLICO
DO ESTADO DA BAHIA

DESPACHO

Sr. Diretor **Carlos Bastos Stucki**,

Cumprimentando-o cordialmente, comunico que autorizo o início do processo licitatório e encaminho-o à DCCL para análise de conformidade e providências posteriores.

Atenciosamente,

Documento assinado eletronicamente por **Yuri Gonzalez Araujo** em 29/07/2021, às 10:32, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.sistemas.mpba.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0165656** e o código CRC **FDF3273B**.

MINISTÉRIO PÚBLICO
DO ESTADO DA BAHIA

DESPACHO

Retorne-se o presente expediente à Diretoria de Tecnologia da Informação informando que, após análise da instrução do processo em epígrafe, identificamos o que segue:

Na instrução do procedimento em geral:

1. Ausência da Comunicação Interna contendo a justificativa da necessidade da contratação por dispensa, conforme estabelece o item 3 do Anexo I - Base de Conhecimento - Dispensas de Licitação - Geral;

2. Ausência da indicação dos servidores que realizarão o acompanhamento do objeto contratado como Fiscal e Suplente, haja vista que não foram informados os respectivos nomes na manifestação da Unidade Gestora, conforme estabelece o item 6.1 do Anexo I - Base de Conhecimento - Dispensas de Licitação - Geral;

3. O orçamento 03 (doc 0164289) está com data de validade próxima do vencimento (30/07/2021). Solicitamos inclusão de orçamento com nova data ou com validade maior, tendo em vista que durante a tramitação do processo a mesma estará vencida. Sugerimos que a validade da proposta seja de, no mínimo, 30 (trinta) dias evitando que o documento vença no curso do processo;

4. No formulário de Informações Orçamentárias (doc 0165242) o campo "Número sequencial da dispensa (Unidade Gestora)" foi preenchido com o nº do processo no SEI. Solicitamos correção do número que deverá ser da própria Unidade Gestora.

Registramos que **os novos documentos deverão ser incluídos após o despacho desta Coordenação e os documentos a serem retificados não deverão ser cancelados do procedimento** de modo a preservar o histórico documental dos documentos anexados ao processo, pois os mesmos são objeto de análise e manifestação de outras unidades administrativas.

Após realização dos ajustes identificados, retorne a esta Unidade.

Coordenação de Elaboração e Acompanhamento de Contratos e Convênios
Diretoria de Contratos, Convênios e Licitações

Documento assinado eletronicamente por **Milena Maria Cardoso do Nascimento** em 02/08/2021, às 09:23, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.sistemas.mpba.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0165739** e o código CRC **3F279D74**.

MINISTÉRIO PÚBLICO
DO ESTADO DA BAHIA

Comunicação Interna nº 2 / DTI - ASSESS SEGURANÇA - COORD - COORDENADOR DE ASSESSORAMENTO EM SEGURANÇA DA INFORMAÇÃO - DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

Em 02 de agosto de 2021.

De: COORDENAÇÃO DE ASSESSORAMENTO EM SEGURANÇA DA INFORMAÇÃO - DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

Para: DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

Assunto:

De: Diretoria de Tecnologia da Informação - CASI

Iaçanã Lima de Jesus Carneiro

Para: Diretoria de Tecnologia da Informação - Diretoria

Yuri Gonzales Araújo

Senhor Diretor,

Solicitamos a V.Sa. autorização e providências para contratação de empresa especialista em Segurança da informação para a Prestação do Serviço de PENTEST - modalidade BLACKBOX, por este Ministério Público , pelo período de por 30 (trinta) dias, na modalidade de dispensa de licitação como forma de atender a demanda urgente advinda da Adminstração Superior de assegurar que a aplicação VOTO DIGITAL foi submetida aos testes técnicos em segurança da informação de que se trata esta contração.

Encaminhamos no presente processo SEI de dispensa de licitação, de toda a documentação necessária pertinente ao referido processo. Esta contratação necessitará de contrato, conforme sinalizado no formulário devido. Informamos, também, segundo documentação de como instruir processo de dispensa no SEI, o nome do fiscal e do suplente:

Iaçanã Lima de Jesus Carneiro - Mat. 351.671

Plinio Andrade Passos - Mat. 354.175

Em tempo, nos colocamos a disposição para esclarecimentos adicionais que se fizerem necessários.

Cordialmente,

Iaçanã Lima de Jesus Carneiro

Coordenador DTI-CASI

Documento assinado eletronicamente por **Iaçanã Lima de Jesus Carneiro** em 02/08/2021, às 11:22, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.sistemas.mpba.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0167064** e o código CRC **91796893**.

PROPOSTA
TÉCNICA COMERCIAL

MINISTÉRIO PUBLICO DA BAHIA

Título: Pentest de Aplicação

Data: 03/08/2021

SFA: 1949964

Versão: 1.0



Sumário

1. VIVO 2
1.1. Institucional 2
1.2. Certificações 2
2. Segurança da Informação 3
2.1 Protegendo a informação 3
2.2 Ameaças Avançadas 4
3. Características do Produto 5
3.1 Metodologia 5
3.2 Enumeração de Vulnerabilidades 6
4. PORTFÓLIO DE EQUIPAMENTOS DE TI E PRESTAÇÃO DE SERVIÇOS 7
4.1 Prestação de Serviços 7
4.2 Teste de Invasão: 8
4.3 Características do Teste 9
4.4 Entregáveis 10
4.5 Limitações 10
5. Condições Gerais de Fornecimento 11
5.1 Responsabilidades Vivo Empresas 12
5.2 Responsabilidades da CONTRATANTE 12
5.3 Premissas 12
5.4 Condições Comerciais Equipamentos TI e Prestação de Serviço 14
5.4.1 Produtos de Revenda 14
5.4.2 Faturamento 14
6. VALIDADE DA PROPOSTA 14
7. CONFIDENCIALIDADE 14
8. ORIENTAÇÕES DIVERSAS 15

Propriedade da Telefônica. Toda e qualquer reprodução, distribuição, comunicação pública é expressamente proibida sem a sua prévia autorização.

SFA769866

Anexo Orcamento 03 (0168072) SEI 19.09.02684.0011790/2021-22 / pg. 168

1. VIVO

1.1. Institucional

A Vivo é a marca comercial da Telefônica Brasil, empresa líder em telecomunicações no País, com 97,8 milhões de acessos (1T18). A operadora atua na prestação de serviços de telecomunicações fixa e móvel em todo o território nacional e conta com um portfólio de produtos completo e convergente para clientes B2C e B2B – banda larga fixa e móvel, ultra banda larga (over fiber), voz fixa e móvel e TV por assinatura. A empresa está presente em 4,3 mil cidades, sendo 4,1 mil com rede 3G e mais de 2,7 mil com 4G, segmento em que é líder de Market Share. A operadora ainda oferece o 4G+, internet duas vezes mais rápida que o 4G. No segmento móvel, a Vivo tem 75,1 milhões de clientes e responde pela maior participação de mercado do segmento (31,9%) no país, de acordo com resultados do balanço trimestral (1T18).

Guiada pela constante inovação e a alta qualidade dos seus serviços, a Vivo está no centro de uma transformação Digital, que amplia a autonomia, a personalização e as escolhas em tempo real dos seus clientes, colocando-os no comando de sua vida digital, com segurança e confiabilidade. A Telefônica Brasil faz parte do Grupo Telefónica, um dos maiores conglomerados de comunicação do mundo, com presença em 21 países, 356,9 milhões de acessos, 122,8 mil colaboradores e receita de 52,0 bilhões de euros em 2017.

Ciente de sua responsabilidade de retribuir à sociedade a confiança que recebe na utilização dos seus serviços, a empresa conta com a Fundação Telefônica Vivo. Desde 1999, a Fundação atua na formação da nova geração, apontando os caminhos para o desenvolvimento do país ao aplicar inovação à educação, empreendedorismo e cidadania, com diferentes projetos sociais nessas áreas.

1.2. Certificações

A **Vivo** utiliza um conjunto de metodologias e melhores práticas reconhecidas pelo mercado para a prestação dos seus serviços.

A empresa tem como política e diretriz empresarial realizar forte investimento em processos e certificações para o aprimoramento da capacitação de seus profissionais e processos internos, melhoria da eficiência e, consequentemente, o aumento da qualidade dos serviços prestados. A **Vivo** entende que o sucesso na implementação dos processos de negócios está baseado em três dimensões: **Atitude**, **Tecnologia** e **Metodologia**.

Propriedade da Telefônica. Toda e qualquer reprodução, distribuição, comunicação pública é expressamente proibida sem a sua prévia autorização.
SFA769866

Anexo Orcamento 03 (0168072) SEI 19.09.02684.0011790/2021-22 / pg. 169

2. Segurança da Informação

2.1 Protegendo a informação

A informação é a alma da empresa moderna. É o seu ativo mais importante e atua como o fator-chave potencializador da atual economia baseada no conhecimento, uma vez que grande parte das atividades diárias dos funcionários requer a criação e o processamento de informação. Assim, proteger os ativos de informação tornou-se uma função-chave para as empresas.

Os serviços de Tecnologia de Informação e Comunicação (TIC) fornecem a infraestrutura necessária para os processos de negócios que permeiam a organização. Em um ambiente altamente competitivo, é fundamental processar a informação de forma eficaz e eficiente, possibilitando protegê-la contra a manipulação não autorizada ou simplesmente inadequada e divulgando-a somente aos recursos-chave que precisam ter acesso a esse conhecimento para realizar as suas tarefas. Ao mesmo tempo, deve-se mantê-la segura e protegida dos olhos curiosos das pessoas que não têm necessidade de acessar essas informações. Este paradigma estabelece um conjunto crescente de exigências de forma a apoiar eficazmente as necessidades dos novos negócios para a acessibilidade de informação que, muitas vezes, extrapola os limites físicos das instalações da empresa. Essa tendência é agravada pela nossa própria necessidade de conectar-nos com os nossos clientes e parceiros de negócios, compartilhar informações e proporcionar novos canais de comunicação.

Ao mesmo tempo, as empresas estão sujeitas a um cenário de ameaças cada vez mais complexo, bem como a pressões reguladoras e padrões industriais de conformidade que requerem um grande nível de especialização e um aumento dos níveis de investimento de capital. Esta tendência não mostra sinais de redução.

Hoje os ataques são direcionados e têm uma motivação financeira. Os tempos em que os malwares eram criados por curiosidade ou para ganhar visibilidade, como uma forma de ganhar fama, já passaram. A maioria destes malwares, também conhecidos como “vírus tradicionais", causavam um grande impacto sobre os recursos de processamento de informações da empresa e podiam ser facilmente descobertos. Hoje, os números são surpreendentes:

- 50 mil novos malwares são detectadas diariamente por empresas de pesquisa de segurança;
- Mais de 200 mil novos sites maliciosos são criados mensalmente.

Os clientes exigem, portanto, que prestadores de serviço reduzam a complexidade inerente a estas realidades, fornecendo soluções e serviços de segurança de custo eficaz que lhes permita concentrar no seu objetivo principal de negócio.

Propriedade da Telefônica. Toda e qualquer reprodução, distribuição, comunicação pública é expressamente proibida sem a sua prévia autorização.
SFA769866

Anexo Orcamento 03 (0168072) SEI 19.09.02684.0011790/2021-22 / pg. 170

2.2 Ameaças Avançadas

Como os ataques estão se tornando cada vez mais sofisticados, o malware foi substituído por outros vetores de ataque. Alguns exemplos dessas novas ameaças incluem:

Botnets	Grupos de computadores infectados controlados remotamente por atacantes maliciosos com objetivo de serem utilizados para coletar informações pessoais, cometer fraudes e roubo de identidade, realizar ataques em massa de negação de serviço em sites e empresas, ou enviar grandes quantidades de e-mail não solicitadas (spam).
Sites legítimos infectados	Os atacantes controlam de forma regular sites de renome usando-os para disseminar malwares clandestinamente para usuários desavisados da web, através de, por exemplo, código malicioso injetado dentro de sites legítimos.
Cross-site scripting (ataques XSS)	Links para sites maliciosos incorporados dentro de outro tipo de conteúdo legítimo para que o usuário web, que acesse um site legítimo, também faça o download do código malicioso hospedado em sites externos ilícitos de maneira automática, sem intervenção ou conhecimento do usuário.
Otimização dos Motores de busca maliciosos (SEO)	A maioria dos usuários conta com motores de busca como Google ou Bing como motores de busca. Os atacantes usam este comportamento contra esses usuários, abusando dos algoritmos que estes motores usam para classificar os resultados. Quando uma notícia de grande repercussão é divulgada, os atacantes produzem rapidamente sites maliciosos sobre tal acontecimento, que promovidos para itens mais bem classificados nos resultados da pesquisa, ficam mais propensos a serem visitados por usuários desavisados que querem saber mais sobre o ocorrido.
Antivírus Falso	Um site malicioso produz um alarme que, para o usuário web, parece um alarme legítimo emitido por um motor antivírus. Este alarme informa o usuário que a sua máquina foi comprometida e que é necessário instalar um antivírus. Quando o usuário concorda, o malware é descarregado para a máquina que passa, então, a ser controlada, tornando-se parte de uma botnet.

Com o tempo, tornam-se cada vez mais comuns este tipo de ameaças sofisticadas. Uma estratégia de proteção eficaz requer mecanismos de adaptação e evolução frente às novas ameaças, mostrando-se como um grande desafio às organizações.

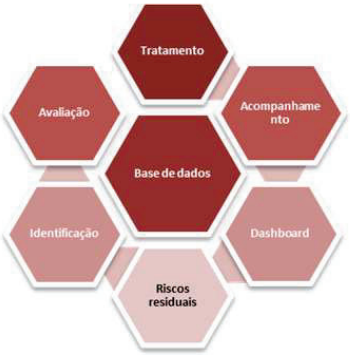
Propriedade da Telefônica. Toda e qualquer reprodução, distribuição, comunicação pública é expressamente proibida sem a sua prévia autorização.
SFA769866

Anexo Orcamento 03 (0168072) SEI 19.09.02684.0011790/2021-22 / pg. 171

3. Características do Produto

3.1 Metodologia

De acordo com o nível de informações que serão passadas sobre o ambiente, o teste pode ser classificado como Black Box (caixa preta), White Box (caixa branca) ou Grey Box (caixa cinza) (híbrido).



Em um teste Black Box, há pouco ou nenhum conhecimento sobre o ambiente a ser avaliado, e tudo deve ser descoberto pelo analista.

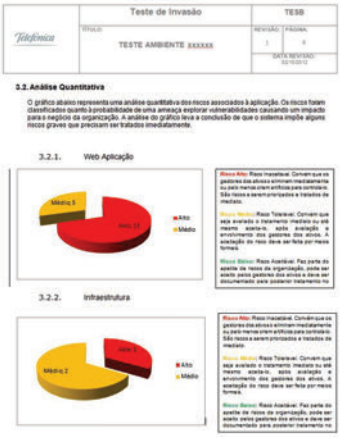
Em testes White Box, analogamente, o avaliador tem acesso irrestrito a qualquer informação que possa ser relevante ao teste, para conduzi-lo supondo o pior cenário, em que o atacante conseguiu obter todos os detalhes sobre o(s) alvo(s).

Dentro do contexto da metodologia de execução de projetos Vivo Empresas, os Testes de Invasão deverão ter escopo bem definido, visando minimizar o potencial de erros durante o processo de simulação de ataque. Também deverão ser formalmente autorizados antes de sua execução, garantindo assim a conformidade legal do projeto.

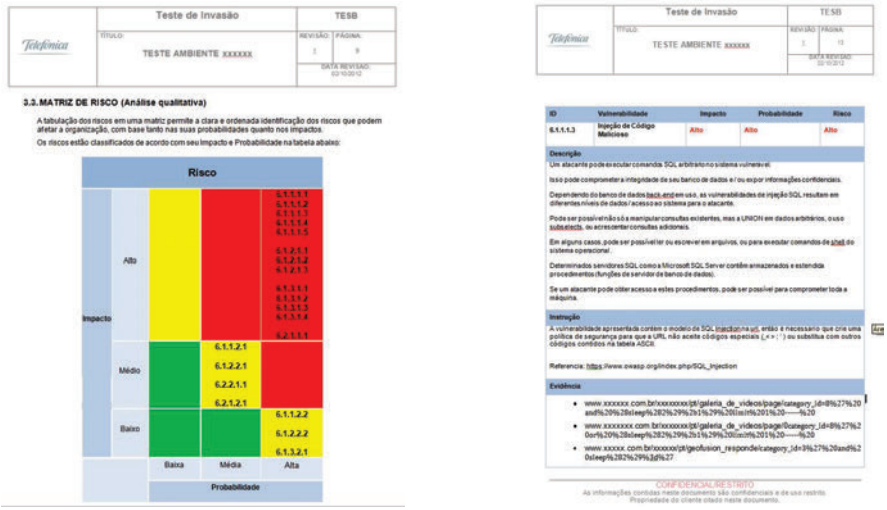
Este trabalho de consultoria tem entre os seus objetivos fornecer orientações estruturadas sobre ações preventivas e corretivas, contribuindo assim para o processo de gestão de Riscos Corporativos e de Segurança da Informação, conforme orientações das normas ABNT/NBR ISO/IEC 27005 e ISO 31000. Sendo assim, nos produtos finais (entregáveis) conterão descrições das vulnerabilidades encontradas, bem como o correspondente grau de risco no contexto onde foram encontradas, bem como orientações sobre procedimentos que poderão ser adotados para corrigir as possíveis falhas encontradas.

Abaixo descrevemos exemplos de relatórios que farão parte dos produtos finais:





Propriedade da Telefônica. Toda e qualquer reprodução, distribuição, comunicação pública é expressamente proibida sem a sua prévia autorização.
SFA769866



Embora o processo de execução das simulações de ataque ocorra com base na experiência de profissionais especializados neste tipo de trabalho, algumas ferramentas são utilizadas para melhor enumeração de vulnerabilidades e avaliações dos riscos associados.

3.2 Enumeração de Vulnerabilidades

Análise de Aplicações Web:

- Injeção de Código Malicioso;
- Cross-site Script (XSS – CSRF);
- Sql Injection;
- Atualização de Sistema (Hardening);
- Enumeração de Diretório;
- Acesso Indevido (Bypass).

Análise de Infraestrutura:

- Atualização do Ambiente (Hardening);
- Acesso Indevido (Bypass);
- Sistemas Habilitados Desnecessários;
- Sistemas Habilitados com versão vulnerável possibilitando Acesso;
- Ataque de Força Bruta (Brute Force).

Propriedade da Telefônica. Toda e qualquer reprodução, distribuição, comunicação pública é expressamente proibida sem a sua prévia autorização.
SFA769866

4. PORTFÓLIO DE EQUIPAMENTOS DE TI E PRESTAÇÃO DE SERVIÇOS

4.1 Prestação de Serviços

Realização de PENTEST de Aplicação Web:

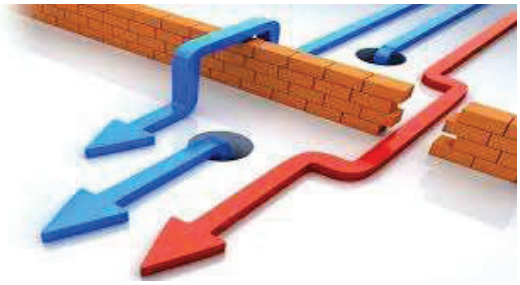
Cliente	Ministério Público da Bahia
Pentest:	Blackbox
Escopo:	Aplicação Web
Estimativa:	30 dias

Blackbox - Ataque externo

A aplicação a ser testada chama-se APLICAÇÃO X, hospedada em 1 servidor web de pequeno porte. Os testes de blackbox externos consistem em simular um cenário de ataque, como qualquer pessoa conectada à Internet, para identificar as violações de segurança existentes no ambiente target que podem colocar em risco as informações processadas e / ou armazenadas lá, ou que pode servir de base para atacar outros ativos tecnológicos do MINISTERIO PUBLICO DA BAHIA.

Propriedade da Telefônica. Toda e qualquer reprodução, distribuição, comunicação pública é expressamente proibida sem a sua prévia autorização.
SFA769866

4.2 Teste de Invasão:



A realização dos testes propostos seguirá as seguintes características:

- Os testes podem ser acompanhados por um responsável da CONTRATANTE;
- O Período de testes, TDI, Coleta de Dados e documentação seguirá conforme Termo de Referência;
- A metodologia utilizada será Blackbox, conforme item 4.1;
- As vulnerabilidades identificadas serão notificadas por meio de relatório técnico, incluindo suas respectivas classificações de risco;
- Serão documentadas e apresentadas as recomendações necessárias para correção dos pontos de vulnerabilidade identificados;
- Entregar e apresentar relatório executivo sobre as vulnerabilidades encontradas.

Propriedade da Telefônica. Toda e qualquer reprodução, distribuição, comunicação pública é expressamente proibida sem a sua prévia autorização.
SFA769866

Anexo Orcamento 03 (0168072) SEI 19.09.02684.0011790/2021-22 / pg. 175

4.3 Características do Teste

Abaixo apresentamos uma visão por fases, para a execução das tarefas planejadas para este projeto, bem como os entregáveis previstos para cada fase:

FASE 01 – PLANEJAMENTO DO PROJETO, ESTABELECIMENTO DE METODOLOGIA E CRITÉRIOS.

Esta fase é obrigatória em todos os projetos de Consultoria em Segurança da Informação da Vivo Empresas, de acordo com a Metodologia de Execução de Projetos. Nesta oportunidade, serão detalhadas todas as atividades, os recursos necessários para sua execução, os prazos estimados para cada atividade e os produtos que deverão ser gerados em cada fase. O cliente deve aprovar o planejamento do projeto, antes que os trabalhos tenham início.

Nesta fase geramos os primeiros Entregáveis do Projeto, que é composto de:

- Relatório de Especificação do Planejamento do Projeto;
- Cronograma detalhado do Projeto;
- Apresentação do Planejamento do Projeto para patrocinadores e outas pessoas envolvidas;

FASE 02 – ANÁLISE DE VULNERABILIDADES DE SEGURANÇA DE REDE E APLICAÇÕES WEB:

Nesta fase, iniciamos as atividades de Pentest em Aplicação Web. Em síntese, esta fase se subdividirá em:

- Análise de Vulnerabilidades de Segurança: Mapeamento de vulnerabilidades e falhas de segurança, em aplicações web e/ou configurações da infraestrutura que suportam o ambiente;
- Apontamento de Recomendações e/ou Oportunidades de Melhorias para a correção destas vulnerabilidades ou mitigação do risco através da implementação de controles de segurança.
- Cobertura das Análises: Os testes contemplarão, no mínimo, 66 testes que estão detalhados no OWASP Testing Guide v4.0. Tais testes serão realizados de maneira automatizada e manual, conforme metodologia definida pela Vivo Empresas para a execução deste projeto.
- Reuniões Intermediárias de apresentação de resultados parciais;
- Apresentação dos Produtos Finais – Resultados dos Testes e Recomendações para cada Vulnerabilidade Encontrada.
- Contempla a realização de Testes de Invasão nos ambientes informados pela CONTRATANTE por Consultor Sênior/Especialista.

Propriedade da Telefônica. Toda e qualquer reprodução, distribuição, comunicação pública é expressamente proibida sem a sua prévia autorização.

SOBRE A EXECUÇÃO DO PROJETO

Deverá ser definida junto a CONTRATANTE a estratégia que será utilizada identificando e definindo os itens que irão compor as atividades do projeto;

Esta proposta não considera a utilização de técnicas que possam causar a indisponibilidade do ambiente, tais como: DDoS, tentativa de exploração automatizada de vulnerabilidades, brute force (em relação à técnica brute force, serão testadas senhas em branco e default);

4.4 Entregáveis

O relatório será entregue por meio seguro, contendo o resultado da avaliação realizada nos ambientes e as vulnerabilidades identificadas durante o teste. Faz parte do relatório apresentar os seguintes conteúdos:

• Sumário Executivo – apresentação de forma resumida do status dos trabalhos e o grau de exposição do ambiente às ameaças de mercado. Este relatório conterá um histórico com a evolução da situação real do ambiente diante das vulnerabilidades, as conclusões do trabalho, bem como as recomendações referentes às vulnerabilidades.

• Descritivo Técnico – será apresentado o resultado da avaliação realizada nos ambientes tecnológicos e as eventuais fragilidades identificadas durante o Teste. O relatório abordará recomendações concretas para correção das vulnerabilidades encontradas. Também será apresentada a priorização para cada vulnerabilidade diagnosticada de acordo com o seu respectivo grau de risco;

4.5 Limitações

Não fazem parte do escopo do trabalho aqui proposto:

- Configuração e/ou manipulação de equipamentos, hardware de propriedades da CONTRATANTE, salvo em atividade de contratação, acordada e autorizada para a execução de PENTESTs;
- Desenvolvimento e correção de código de software, arquiteturas de bancos de dados como entregas de projeto, entre outros.
- Responsabilização para a Vivo Empresas em processo de seleção de empresas. A indicação de empresas prestadoras e fornecedores de solução é um serviço de consultoria com vistas facilitação e aconselhamento nos trabalhos a serem executados. A responsabilidade pelo

Propriedade da Telefônica. Toda e qualquer reprodução, distribuição, comunicação pública é expressamente proibida sem a sua prévia autorização.

Anexo Orcamento 03 (0168072) SEI 19.09.02684.0011790/2021-22 / pg. 177

processo de requerimento por proposta para empresas indicadas ou não, seleção e compra de solução ficam reservados, única e exclusivamente ao CONTRATANTE, seus profissionais e seus processos internos.

- Elaboração de Normas específicas de segurança da informação e/ou procedimentos de segurança de qualquer natureza não ligados ao ambiente da proposta;
- Correção de vulnerabilidades encontradas durante a realização dos trabalhos;
- Implementação ou manipulação de regras em firewall, IPS, IDS, roteadores, switches e/ou sistemas de informação e segurança de qualquer natureza;
- Análise de segurança lógica em outros sistemas de computadores e redes de comunicação não destacados no escopo;
- Análises de segurança de aplicações corporativas, suas especificações e suas funcionalidades fora do âmbito do escopo;
- Análise de segurança dos bancos de dados nos aspectos de modelagem e estruturação de seus databases de aplicação;
- Avaliação, fornecimento e implementação de ferramentas que eventualmente sejam recomendadas pela análise de vulnerabilidades, nem de outras ferramentas que venham a ser necessárias;
- Execução de atividades ligadas à Ethical Hacking (ETH) ou outros formatos e métodos de avaliação de vulnerabilidades tipo manual;
- Atendimento a demandas que envolvam trabalho fora do horário comercial. Se surgirem necessidades deste tipo, a Vivo Empresas deverá ser formalmente comunicada, a fim de que um plano de trabalho possa ser avaliado e aprovado pelas partes, atendendo assim a legislação trabalhista vigente.

5. Condições Gerais de Fornecimento

As partes concordam que as suas equipes profissionais lhes são necessárias para o desempenho das suas atividades e execução do projeto. Assim, durante a vigência do mesmo e até 1 (um) ano após o seu término, nenhuma das partes contratará direta ou indiretamente qualquer profissional que tenha mantido contrato com a outra parte nos 12 (doze) meses precedentes.

No caso de violação do aqui disposto, a parte infratora ficará obrigada a pagar à outra parte a importância equivalente ao total pago ao profissional indevidamente recrutado nos doze últimos meses de vínculo com a parte lesada.

Propriedade da Telefônica. Toda e qualquer reprodução, distribuição, comunicação pública é expressamente proibida sem a sua prévia autorização.
SFA769866

Anexo Orcamento 03 (0168072) SEI 19.09.02684.0011790/2021-22 / pg. 178

5.1 Responsabilidades Vivo Empresas

A Vivo Empresas se compromete a executar os serviços propostos observando rigorosamente as condições ajustadas em relação a padrões, prazos e produtos.

A Vivo Empresas e seus prepostos se comprometem a dar tratamento confidencial aos fatos e informações reservadas aos quais tiverem acesso no decorrer dos trabalhos. Após a aprovação da presente proposta a Vivo Empresas designará um gerente de projetos a fim de atuar como responsável pelos serviços junto ao CONTRATANTE.

5.2 Responsabilidades da CONTRATANTE

É responsabilidade da CONTRATANTE, designar os seus representantes na equipe do projeto, com a disponibilidade necessária para participar de todas as atividades previstas no plano de trabalho.

A CONTRATANTE deverá manter total confidencialidade em relação às técnicas, instrumentos e metodologias aplicados pela Vivo Empresas na prestação dos serviços objeto desta proposta.

Mudanças nos sistemas e ferramentas de TI, equipes internas e/ou nas atividades da CONTRATANTE que porventura venham a ocorrer serão objeto de negociação complementar entre as partes, sempre que estas mudanças demandarem carga horária complementar relacionadas com a revisão das atividades e da documentação já elaborados e apresentados à CONTRATANTE.

Muitos dos nomes de serviços e de empresas referidas neste documento são marcas registradas. Todas elas são reconhecidas mediante esta declaração.

Neste período, o planejamento de projeto deverá cobrir todos os gaps de requisitos nos quais a Vivo Empresas se predispõe e coloca à disposição os profissionais designados para atender o requerido no planejamento de projeto.

Atrasos provocados na contratação de fornecedores e soluções e/ou no fornecimento e/ou implementações, correções, etc, provocados por terceiros ou a própria CONTRATANTE não poderão onerar o tempo de contratação, ficando a Vivo Empresas isenta de responsabilização por tais atrasos.

5.3 Premissas

As seguintes premissas são consideradas para que a prestação dos serviços ocorra da forma esperada:

- Não será empregado qualquer técnica ou artifício que envolva engenharia social, como envio de mensagens de e-mail contendo phishing, mensagens do tipo SMS ou ligações telefonicas com ID reais ou forjadas para obteção de informações;

Propriedade da Telefônica. Toda e qualquer reprodução, distribuição, comunicação pública é expressamente proibida sem a sua prévia autorização.

- Nos cenários de testes de infraestrutura externa, todos os testes e tentativas serão realizados de forma remota;
- Não está previsto qualquer atuação interna de forma presencial ou remota através de VPN/dispositivos de acesso remoto;
- O início das atividades contratadas está condicionado com a realização de um kickoff entre as equipes da Vivo Empresas S/A e o cliente e com o preenchimento e assinatura do Termo de Autorização;
- Não está previsto a análise de qualquer aplicativo móvel relacionado a empresa, ao sistema ou URL a ser analisada;

Propriedade da Telefônica. Toda e qualquer reprodução, distribuição, comunicação pública é expressamente proibida sem a sua prévia autorização.
SFA769866

Anexo Orcamento 03 (0168072) SEI 19.09.02684.0011790/2021-22 / pg. 180

5.4 Condições Comerciais Equipamentos TI e Prestação de Serviço

5.4.1 Produtos de Revenda

Os preços dos serviços constantes nesta proposta estão expressos em Reais refletem os impostos, taxas, contribuições vigentes na época da confecção desta Proposta. Caso haja alguma alteração para mais ou para menos destas condições, incluído a supressão ou adição de novos impostos, taxas, a Vivo Empresas se reserva no direito de efetuar os devidos ajustes de preços correspondentes.

Item	Descrição do Serviço	Valor à Vista c/ impostos
01	Pentest de Aplicação (30 dias)	R$ 41.186,85

5.4.2 Faturamento

O faturamento/cobrança dos serviços será à vista com vencimento em 30 dias a partir da data de emissão da Nota Fiscal.

ESTEIRA DE FATURAMENTO

- Faturamento T-Bra - Telefônica Brasil S.A

6. VALIDADE DA PROPOSTA

Os preços apresentados nesta Proposta são válidos por 10 (dez) dias contados a partir da data de sua entrega, salvo alterações macro ou microeconômicas significativas na economia do país.

7. CONFIDENCIALIDADE

A Vivo está ciente que as informações contidas comerciais neste documento são confidenciais e não deverão ser divulgadas fora do âmbito desta. O cliente autoriza a Vivo utilizar suas informações, tanto cadastrais quanto de perfil de consumo de tráfego, para análises internas.

Desde já aceita e concorda que a Vivo poderá dar publicidade do presente Projeto, a qualquer tempo, em mídia impressa e eletrônica, no território brasileiro ou fora dele, exclusivamente para divulgação de case, sem que se caracterize uso indevido de marca, nome comercial, imagem e/ou de quaisquer direitos do Cliente.

Propriedade da Telefônica. Toda e qualquer reprodução, distribuição, comunicação pública é expressamente proibida sem a sua prévia autorização.
SFA769866

Anexo Orcamento 03 (0168072) SEI 19.09.02684.0011790/2021-22 / pg. 181

8. ORIENTAÇÕES DIVERSAS

Este documento é uma proposta comercial. A contratação do serviço ficará pendente da assinatura do contrato.

Só serão aceitas solicitações de serviços que forem devidamente acompanhadas do Contrato social e Procuração da pessoa que assinou o presente instrumento. Será necessário informar os Cartórios para reconhecimento de firma do Cliente.

IMPORTANTE: Es Sumário Executivo/Proposta Comercial, o Termo de Contratação/Formulário e seus anexos estão sujeitos a viabilidade técnica.

Propriedade da Telefônica. Toda e qualquer reprodução, distribuição, comunicação pública é expressamente proibida sem a sua prévia autorização.
SFA769866

Anexo Orcamento 03 (0168072) SEI 19.09.02684.0011790/2021-22 / pg. 182

São Paulo, 03 de agosto de 2021

A/C MINISTERIO PUBLICO DA BAHIA,

A Vivo é uma empresa que conhece as necessidades específicas de seus clientes e oferece as soluções mais avançadas em telecomunicações e serviços digitais com o melhor custo-benefício.

Agradecemos a oportunidade de apresentar esta proposta para a prestação de nossos serviços adequando às necessidades da sua empresa.

Antecipadamente nos colocamos à sua disposição para esclarecer ou revisar quaisquer itens a seguir descritos, para que a nossa proposta esteja plenamente alinhada com as suas necessidades.

Atenciosamente,

Emília Pitanga Sampaio Mettig
Diretoria de Governo | Gerencia Governo FSP
Gerente de Negocios – Especialista Governo
Tel.: (071) 99980-2026
Rua Silveira Martins, nº1036, Módulo 6, Cabula,
Salvador (BA), Cep.:41150-000
emilia.mettig@telefonica.com

Cristiane Soares Nunes Couto
Gerente Negócios Serviços Digitais
Div. Serviços Digitais
Cel + 55 11 95665- 9246
Av. Engenheiro Luis Carlos Berrini, 1376 – 28° Andar
04571-000 | São Paulo – SP
cristiane.couto@telefonica.com

Lival Estrela
Consultor de Soluções e Negócios | Pré-Vendas Gov. Federal e Regionais | PWF#F02
Diretoria de Produtos, Pré-Vendas e Pós-Vendas | Telefônica Brasil
Rua Silveira Martins 1036, Módulo 6, 1 andar
CEP 41150-000 | Salvador - BA
Cel + 55 71 99980-2365
lival.estrela@telefonica.com

Propriedade da Telefônica. Toda e qualquer reprodução, distribuição, comunicação pública é expressamente proibida sem a sua prévia autorização.
SFA769866

MINISTÉRIO PÚBLICO
DO ESTADO DA BAHIA

MANIFESTAÇÃO

Informamos para os devidos fins que foram atendidos os pontos 1,2 e 3 elencados do despacho da DCCL. As informações referente ao ponto 1 e 2 estão em nossa CI. O ponto do referido despacho refere-se a informações orçamentárias.

Atenciosamente.

Documento assinado eletronicamente por **Iaçanã Lima de Jesus Carneiro** em 02/08/101, à9s , , :20àcon3rme artf , .à‰àl" Iàda bei , , fL, 4/1006f

A autenticidade do documento pode ser con3rida no site https://seifsistemasfmp" afmpf" r/sei/controlador_externofphp?acao=documento_con3rir&id_orgao_acesso_externo=0 in3rmando o código veri3cador **0168090** e o código CRC **49BB7334**f

Informações Orçamentárias - 0169176

Formulário de Informações Orçamentárias

Projeto / Ação / Atividade (número e nome):
2002 - MANUTENÇÃO DE SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Código da Unidade Orçamentária:
40601

Código da Unidade Gestora:
0003

Saldo Orçamentário:
R$ 2.149.795,28

Natureza da Despesa:
33.90.40

Responsável pela Informação:
JORGE ALBERTO DOS SANTOS CONCEIÇÃO

Responsável pela Unidade Gestora:
YURI GONZALEZ ARAÚJO

Número Sequencial da Dispensa / Inexigibilidade (Unidade Gestora):
004

Do/ umento assinado eletroni/ amente cor **Jorge Alberto dos Santos Conceicao** em 04p08p2021, às 13:46, / onforme art. 1º, III, "b", da Lei 11.419p2006.

A autenti/ idade do do/ umento code ser / onferida no site httcs:ppsei.sistemas.mcba.mc.brpseip/ ontrolador_externo.chc?a/ ao=do/ umento_/ onferir&id_orgao_a/ esso_externo=0 informando o / ódigo verifi/ ador **0169176** e o / ódigo CRC **B97A8AD7**.

MINISTÉRIO PÚBLICO
DO ESTADO DA BAHIA

MANIFESTAÇÃO

Prezados, bom dia!

Cumprimentando-os cordialmente, encaminho o **PROCESSO SEI Nº 11790/2021 - DISPENSA DE LICITAÇÃO,** com as Informações Orçamentárias devidamente **SANEADAS**, quanto ao atendimento ao Item 4 do Despacho da DCCL, estando o Processo **APTO** para o seu prosseguimento regular.

Atenciosamente.

Jorge Alberto dos santos Conceição

Assistente Técnico Administrativo

Diretoria de Tecnologia da Informação - DTI

Execução Orçamentária

Documento assinado eletronicamente por **Jorge Alberto dos Santos Conceicao** em 02/08/101, à9s , : 3?f àcon.orme artº , Ià""àtLbàda 4ei , , º2, 6/100f º

A autenticidade do documento pode ser con.erida no site https3/seiºsistemasºmpLaºmpºLr/sei/controlador_externoºphp?acao=documento_con.erir&id_orgao_acesso_externo=0 in.ormando o código veri.icador **0169179** e o código CRC **D679FAEA**º

1º Traslado
LIVRO N° 0290
PÁGINA 159/165

PROCURAÇÃO BASTANTE QUE FAZ: **ORBITALL SERVIÇOS E PROCESSAMENTO DE MEIOS DE PAGAMENTO LTDA e outros**

SAIBAM quantos este público instrumento de procuração bastante virem que, **aos trinta e um (31) dias do mês de maio do ano de dois mil e vinte e um (2021),** neste Oficial do Registro Civil das Pessoas Naturais do 39º Subdistrito Vila Madalena, por vídeoconferência nos termos do Provimento 100 do CNJ, perante mim, SUBSTITUTA, compareceram como outorgantes: **1) ORBITALL SERVIÇOS E PROCESSAMENTO DE MEIOS DE PAGAMENTO LTDA**, sociedade empresária limitada, inscrita no CNPJ sob nº 14.550.922/0001-87, com sede na Rua Elpidio de Almeida, nº 1111, bloco K, Catolé, Campina Grande-PB, filial inscrita no CNPJ/ME sob nº 14.550.922/0002-68 localizada na Rua Alfredo Pujol, 506, Santana, São Paulo - SP, com seu Instrumento Particular de 4ª Alteração do Contrato Social Consolidado, datado de 02/12/2013, devidamente registrado na Junta Comercial do Estado de São Paulo (JUCESP) em 18/12/2013, sob o nº 479.664/13-4 e pela Junta Comercial do Estado da Paraíba, aos 07/01/2014, sob nº 25200621174 e Certidão Simplificada Eletrônica, emitida pela Junta supramencionada aos 13/05/2021, código nº MSU1QPIP, neste ato representada nos termos da CLÁUSULA 4ª - ADMINISTRAÇÃO, ITENS 4.1, 4.4 e 4.7, do documento supracitado, cuja cópia fica arquivada nesta Serventia em Pasta Própria (CS 74, fls. 71), pelos Diretores eleitos conforme Ata de Reunião de Sócios, realizada aos 28/06/2018, devidamente registrada na Junta Comercial do Estado da Paraiba aos 21/08/2018, sob o nº 20180819356: **MARCO ANTONIO SILVA STEFANINI,** [redacted] **MARIA DAS GRAÇAS VUOLO SAJOVIC STEFANINI,** [redacted] **2) STEFANINI CONSULTORIA E ASSESSORIA EM INFORMÁTICA S.A.,** sociedade anônima, inscrita no CNPJ sob nº 58.069.360/0001-20, com sede na Avenida Jaguary, 164, Centro, Jaguariúna-SP, com seu Estatuto Social anexo a Ata de Assembleia Geral Extraordinária, realizada aos 29/10/2019, devidamente registrada na Junta Comercial do Estado de São Paulo (JUCESP) em 04/12/2019, sob o nº 619.848/19-4 e Certidão Simplificada Eletrônica, emitida pela Junta supramencionada, aos 16/04/2021, sob nº de autenticidade 150427530, neste ato representado nos termos dos ARTIGOS 13 e 20, do documento supracitado, cuja cópia fica arquivada nesta serventia em pasta própria (CS 83, fls 08), pelos diretores eleitos conforme Ata da Assembleia Geral Extraordinária, realizada em 18/07/2018, devidamente registrada na Junta Comercial do Estado de São Paulo (JUCESP) em 07/08/2018, sob o nº

Esse documento foi assinado por GABRIELA DA AFRICA LAPA.
Para validar o documento e suas assinaturas acesse https://assinatura.e-notariado.org.br/validate e informe o código UFRD8-446GZ-NG9J7-QCXP9
e-notariado
Anexo Procuracao (0169642) SEI 19.09.02684.0011790/2021-22 / pg. 187

370.988/18-8: **MARCO ANTONIO SILVA STEFANINI,** [redacted] e **MARIA DAS GRAÇAS VUOLO SAJOVIC STEFANINI,** [redacted] **3) STEFANINI RAFAEL SEGURANÇA E DEFESA S.A.**, sociedade anônima, inscrita no CNPJ/MF de nº 24.691.488/0001-09, com sede na Avenida Eusébio Matoso, 1375, 8º andar, salas 801 e 802, Butantã, CEP 05423-905, São Paulo, SP, com seu Estatuto Social Consolidado, anexo a Ata da Assembleia Geral Extraordinária, realizada aos 09/01/2017, devidamente registrada na Junta Comercial do Estado de São Paulo (JUCESP) aos 24/02/2017, sob nº 106.436/17-0 e Certidão Simplificada Eletrônica, emitida pela Junta supramencionada, aos 16/04/2021, autenticidade nº 150428367, neste ato representada nos termos dos ARTIGOS 13, 18 - Parágrafo 1º, 19 - Parágrafo 1º, do documento supracitado, cuja cópia fica arquivada nesta Serventia em Pasta Própria (CS 70, fls. 58), pelos Diretores eleitos conforme Instrumento Particular de 1ª Alteração ao Contrato Social e Assembleia Geral de Transformação, datado de 10/05/2016, devidamente registrado na Junta Comercial do Estado de São Paulo (JUCESP), aos 24/06/2016, sob nº 3530049265-0: **MARCO ANTONIO SILVA STEFANINI**, [redacted] **MARIA DAS GRAÇAS VUOLO SAJOVIC STEFANINI**, [redacted] **4) STEFANINI NETWORKING CONSULTORIA DE INFORMÁTICA LTDA.**, sociedade empresária limitada, inscrita no CNPJ sob nº 01.530.329/0001-27, com sede na Avenida Deputado Cristovam Chiaradia, 670, loja 01, Buritis, Belo Horizonte - MG, com seu Instrumento Particular de 38ª Alteração do Contrato Social Consolidada, datada de 20/10/2020, devidamente registrada na Junta Comercial do Estado de Minas Gerais (JUCEMG) em 12/11/2020, sob o nº 8091549 e Certidão Simplificada Eletrônica, emitida pela Junta supramencionada, aos 22/04/2021, código nº C210000903411, neste ato representada nos termos do ARTIGO 6º - Parágrafos 2º 3º e 4º do documento supracitado cuja cópia fica arquivada nesta Serventia em Pasta Própria (CS 83, fls 09), pelos Administradores: **MARCO ANTONIO SILVA STEFANINI**, [redacted] e **MARIA DAS** [redacted] e **5) ORBITALL ATENDIMENTO LTDA**, sociedade empresária limitada, inscrita no CNPJ sob nº 18.081.219/0001-28, com sede na Rua Elpídio de Almeida, 1111, Catolé, Campina Grande - PB, filial inscrita no CNPJ/ME sob nº 18.081.219/0003-90 localizada na Rua Alfredo Pujol, 506, andar 4, Santana, São Paulo - SP, com seu Instrumento de 8ª Alteração e Consolidação do Contrato Social, datado de 01/09/2020, devidamente registrada na Junta Comercial do Estado da Paraíba, aos

Esse documento foi assinado por GABRIELA DA AFRICA LAPA.
Para validar o documento e suas assinaturas acesse https://assinatura.e-notariado.org.br/validate e informe o código UFRD8-446GZ-NG9J7-QCXP9
e-notariado
Anexo Procuracao (0169642) SEI 19.09.02684.0011790/2021-22 / pg. 188

17/09/2020, sob nº 20204225000 e Certidão Simplificada Eletrônica emitida pela Junta supracitada aos 13/05/2021, código nº XFLAOFEF, neste ato representada nos termos dos ARTIGO 6º, PARÁGRAFOS 4º, 5º e 6º, do documento supracitado, cuja cópia fica arquivada nesta serventia em pasta própria (CS 78, fls. 88), pelos Diretores: **LUIZ ANTONIO BASTOS IANNINNI,** [redacted] e **MARIA** [redacted]; reconhecidas por mim SUBSTITUTA, com base na documentação de identidade exibida e supra mencionada; e então, por elas me foi dito que; por este público instrumento e nos termos de direito nomeiam e constituem seus bastantes procuradores: **LUIZ CARLOS MARQUES DE AGUIAR,** [redacted] e **MARIA MAGALI** [redacted]; a quem confere os poderes "Ad-Negotia", para representar as Outorgantes em Juízo e fora dele, nas suas atividades, obedecendo a seguinte forma: **A-) AGINDO EM CONJUNTO COM UM DIRETOR OU OUTRO PROCURADOR DEVIDAMENTE CONSTITUÍDO**, para: **i-)** representá-la perante quaisquer Bancos, inclusive Caixa Econômica ou outra entidade do Sistema Financeiro Nacional, inclusive Banco Itaú S/A., Banco Bradesco S/A, Caixa Econômica Federal, Unibanco, Citibank, Nossa Caixa S/A, Banco HSBC, Banco Santander, Bank Boston S/A., Banco do Brasil S/A., Banco Central do Brasil, Sicredi e em demais estabelecimentos bancários e de crédito, financiamento e investimentos, cooperativas de crédito, assinar contratos de arrendamento mercantil, podendo abrir, movimentar e encerrar contas correntes e de investimento; fazer depósito e saques, aplicações e resgates, emitir, pagar, receber, aceitar, reformar, caucionar, avalizar, endossar e descontar, sempre a ordem da Outorgante, cheques, ordens de pagamento, duplicatas, notas promissórias, letras de câmbio e quaisquer outros títulos de crédito, solicitar saldos, extratos e talões de cheques, assinar borderôs, contratos de mútuo, de câmbio e outros que interessem a Outorgante, no que tange às suas operações, ajustando termos, cláusulas e condições; **ii-)** representá-la perante quaisquer pessoas físicas ou jurídicas, públicas ou privadas, podendo contratar, compromissar, adquirir, alienar, pagar e transferir por qualquer meio, bens móveis, mercadorias, receber e dar quitação, confessar, acordar, transigir a respeito de qualquer assunto ou ato comercial, financeiro, direito ou obrigação, relativos aos negócios sociais da Outorgante, para desenvolvimento de suas atividades; **iii-)** representá-la perante Oficiais de Registro de Imóveis, cartórios de Notas, podendo assinar escrituras, dar e receber quitação, pagar impostos, contribuições, taxas e emolumentos, **SENDO VEDADO O SUBSTABELECIMENTO DOS PODERES DO ITEM "A", ACIMA RELACIONADOS; B-) AGINDO ISOLADAMENTE: i-)** para praticar atos em nome da Companhia, podendo assinar requerimentos, contratos de arrendamento mercantil, receber citações judiciais, levantar depósitos recursais e judiciais, prestar depoimentos em qualquer Juízo, como representante legal da Outorgante nas suas atividades, assinar cartas, contratos de trabalho, admitir, demitir

Esse documento foi assinado por GABRIELA DA AFRICA LAPA.
Para validar o documento e suas assinaturas acesse https://assinatura.e-notariado.org.br/validate e informe o código UFRD8-446GZ-NG9J7-QCXP9
e-notariado
Anexo Procuracao (0169642) SEI 19.09.02684.0011790/2021-22 / pg. 189

e suspender empregados, conceder férias, baixar instruções e ordens de serviços, assinar CTPS e fazer respectivas anotações; **ii-)** perante empresas públicas, de economia mista, autarquias, concessionárias de serviços públicos, cooperativas, incluindo Sicredi, associações da classe, sindicatos, Repartições Públicas Federais, Estaduais e Municipais, inclusive Receita Federal do Brasil, para emissão de guia do parcelamento da Receita Federal do Brasil, para confissão de dívida, solicitar parcelamento ou desistência de parcelamento, renegociação, e negociação, de impostos federais e previdenciários junto à Receita Federal do Brasil, Procuradoria Geral da Fazenda Nacional, INSS, Caixa Econômica Federal, Banco Central do Brasil, Registros Públicos, Juntas Comerciais, Consulados e Embaixadas, Delegacias de Polícia ou do Trabalho, Órgãos Fiscais, fazendeiros e alfandegários em geral, secretaria da fazenda, CACEX, Empresa Brasileira de Correios e Telégrafos, Bolsa de Valores, podendo receber, retirar, assinar e apresentar quaisquer documentos, correspondências, impressos e prestar quaisquer esclarecimentos necessários, podendo propor contra quem de direito as ações competentes e defendê-lo nas contrárias, seguindo umas e outras até final decisão, usando para tanto de todos os recursos legais e processuais e acompanhá-los, conferindo-lhe poderes especiais para transigir, confessar, reconhecer a procedência do pedido, desistir, renunciar ao direito, receber e dar quitação, solicitar informações e documentos, assinar autorização, para movimentação de conta vinculada ao FGTS - Fundo de garantia por tempo de Serviço, assinar guias, livros, e requerimentos; **iii-)** perante quaisquer pessoas jurídicas de direito público ou privado, todos seus órgãos, departamentos, seções, Instâncias, empresas públicas, de economia mista, autarquias, concessionárias de serviços públicos, cooperativas, Sicredi, associações da classe, sindicatos, Repartições Públicas Federais, Estaduais, Municipais, inclusive Receita Federal do Brasil, Procuradoria Geral da Fazenda Nacional, INSS, Caixa Econômica Federal, Banco Central do Brasil, Registros Públicos, Juntas Comerciais, Consulados e Embaixadas, Delegacias de Polícia ou do Trabalho, Órgãos Fiscais, Fazendários, ou Alfandegários em geral, Secretaria da Fazenda, CACEX, Empresa Brasileira de Correios e Telégrafos, Bolsa de Valores, Prefeituras Municipais, para participar de concorrências e licitações públicas, podendo assinar, requerer, apresentar quaisquer informações, documentos e propostas, participar de sessões públicas de abertura de documentação de habilitação e de propostas, assinar as respectivas atas, registrar ocorrências, formular impugnações, reclamações, propostas, interpor recursos, renunciar ao direito de recursos, fazer novas propostas, rebaixar preços, conceder descontos, prestar caução, levantá-las, receber as importâncias caucionadas ou depositadas, transigir, desistir e praticar todos os atos e assinar todos os documentos indispensáveis ao bom e fiel cumprimento do presente mandato, podendo ainda assinar termo de compromisso e/ou constituição de consórcio bem como o termo de consórcio em si; **iv-)** perante quaisquer pessoas físicas e jurídicas de direito público ou privado, assinar contratos em geral, convênios, acordo de confidencialidade, contrato de locação, contrato de prestação e/ou contratação de serviços, inclusive relativas a instruções sobre títulos, autorizar abatimentos, descontos e prorrogações de vencimento, forma de pagamento, protestos; **v-)** podendo ainda assinar relatórios, declarações e demonstrativos contábeis e financeiros de suas atividades; **vi-)** constituir advogados conferindo-lhes os poderes da cláusula "Ad-Judicia", para o for em geral, em qualquer Juízo, Instância ou Tribunal, podendo ainda confessar, transigir, desistir, alterar a natureza da ação, fazer acordos, nomear prepostos para ações trabalhistas, dar e aceitar quitação. **PODENDO INCLUSIVE SUBSTABELECER OS PODERES ACIMA MENCIONADOS**. **A PRESENTE PROCURAÇÃO TERÁ VALIDADE DE 01 (UM) ANO A CONTAR DESTA DATA**. **Os**

Esse documento foi assinado por GABRIELA DA AFRICA LAPA.
Para validar o documento e suas assinaturas acesse https://assinatura.e-notariado.org.br/validate e informe o código UFRD8-446GZ-NG9J7-QCXP9
e-notariado
Anexo Procuracao (0169642) SEI 19.09.02684.0011790/2021-22 / pg. 190

elementos relativos à qualificação e identificação dos procuradores, bem como o objetivo do presente mandato foram fornecidos e conferidos pelos representantes das outorgantes, que por eles se responsabilizam. Os representantes das outorgantes declaram que não houveram alterações estatutárias posteriores às supramencionadas. E, de como assim o disse, do que dou fé, lavrei este público instrumento que sendo-lhe lido, aceita. Eu, **GABRIELA DA AFRICA LAPA**, **SUBSTITUTA**, a lavrei (assinatura digital) **MARCO ANTONIO SILVA STEFANINI | MARIA DAS GRAÇAS VUOLO SAJOVIC STEFANINI | LUIZ ANTONIO BASTOS IANNINNI | GABRIELA DA AFRICA LAPA**. (Desta: R$ 310,60: Guia nº 023/2021). Esta legalmente selada. Trasladada a seguir conferindo com o original. Nada mais, dou fé. Eu, **GABRIELA DA AFRICA LAPA, SUBSTITUTA,** conferi, subscrevo, dou fé e assino em público e raso.

Em Testemunho _____ Da Verdade.

Assinado digitalmente por:
GABRIELA DA AFRICA LAPA
CPF: [redacted]
Certificado emitido por AC Certisign RFB G5
Data: 05/06/2021 09:21:24 -03:00

Colégio Notarial do Brasil CONSELHO FEDERAL

_____

GABRIELA DA AFRICA LAPA
SUBSTITUTA

Selo digital n°: 1132411TR000000009709421V Valor: R$ 0,00
Para conferir a procedência deste documento efetue a leitura do QR Code impresso ou acesse o endereço eletrônico https://selodigital.tjsp.jus.br.

Esse documento foi assinado por GABRIELA DA AFRICA LAPA.
Para validar o documento e suas assinaturas acesse https://assinatura.e-notariado.org.br/validate e informe o código UFRD8-446GZ-NG9J7-QCXP9
e-notariado

MANIFESTO DE ASSINATURAS

Código de validação: UFRD8-446GZ-NG9J7-QCXP9

Matrícula Notarial Eletrônica: 113241.2021.05.31.00000072-73

Esse documento foi assinado pelos seguintes signatários nas datas indicadas (Fuso horário de Brasília):

✔ GABRIELA DA AFRICA LAPA (CPF 344.584.838-62) em 05/06/2021 09:21

Para verificar as assinaturas acesse https://assinatura.e-notariado.org.br/validate e informe o código de validação ou siga o link a abaixo:

https://assinatura.e-notariado.org.br/validate/UFRD8-446GZ-NG9J7-QCXP9

MINISTÉRIO PÚBLICO
DO ESTADO DA BAHIA

MANIFESTAÇÃO

Informamos para os devidos fins que foram realizados os saneamentos por esta Coordenação dos expostos em despacho e e-mail da DCCL, onde nos foi solicitado incluir o documento de procuração da empresa. Informo também que as informações solicitadas referentes a saneamentos em relação a parte orçamentária foram anexadas pelo nosso Apoio Técnico.

Assim segue o este processo de dispença para sua devida trâmitação.

Cordialmente,

Documento assinado eletronicamente por **Iaçanã Lima de Jesus Carneiro** em 05/08/2021, às 09:41, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.sistemas.mpba.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0169644** e o código CRC **DC0CC594**.

MINISTÉRIO PÚBLICO
DO ESTADO DA BAHIA

MANIFESTAÇÃO

Sr. Diretor **Carlos Bastos Stucki**,

Cumprimentando-o cordialmente, ratifico a autorização o processo licitatório e encaminho-o à DCCL após saneamento realizado por essa DTI.

Atenciosamente,

Documento assinado eletronicamente por **Yuri Gonzalez Araujo** em 11/08/2021, às 13:27, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.sistemas.mpba.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0173505** e o código CRC **09ACDBF8**.

MINISTÉRIO PÚBLICO
DO ESTADO DA BAHIA

DESPACHO

Encaminhamos o procedimento à Unidade demandante, após o saneamento preliminar do mesmo, indicando a necessidade de alguns ajustes/esclarecimentos a seguir:

Na instrução do procedimento em geral:

1. Recomendamos, como já sinalizado em outras oportunidades e como, ademais, é recomendado para tramitação de procedimentos informatizados em geral, que, uma vez encaminhado o procedimento a outra unidade, seja o mesmo concluído na unidade remetente, de modo a manter tramitação regular e semelhante à forma física, evitando, assim, a alteração do fluxo procedimental mediante a inserção de documentos/manifestações extemporâneos e concomitantes com diligências realizadas na unidade em que se encontra o processo. Ressaltamos que, caso a unidade pretenda acompanhar o andamento do procedimento, há o recurso "acompanhamento especial" especificamente desenvolvido para tanto.

2. Sugerimos que, no formulátio "Dispensa de Licitação - Formulário de Autorização/Solicitação", sejam informados os nomes e valores dos itens conforme ordem descrescente de preços, de modo que o fornecedor 1 seja aquele que apresentou o valor mais baixo para a contratação pretendida.

3. Verificamos que na Procuração constante no procedimento (0169642) Maria Magali Bredariol, cujo documento de identidade se encontra no expediente (0165289), tem poderes outrogados apenas pela empresa ORBITALL ATENDIMENTO LTDA. Além da referida outrorgante não ser a empresa indicada como contratada, a supracitada Procuradora somente poderia agir em conjunto com um Diretor ou com outro Procurador devidamente constituído no que diz respeito à representação da empresa em contratações com pessoas físicas ou jurídicas.

No Documento de Oficialização da Demanda:

4. No item 2.3 e 2.4 do Anexo ao DOD, informa-se que a Contratada permanecerá, durante todo o prazo de execução, qual seja, 30 dias, realizando diversos testes. Compreendemos, dete modo, que os serviços serão realizados de maneira contínua, dentro do prazo de execução dos mesmos, com entregas periódicas de relatórios dos testes realizados. Neste sentido, e considerando que havia previsão na contratação anterior, conforme indicado abaixo, solicitamos esclarecimento acerca da necessidade ou não de definição de prazos para entregas periódicas dos relatórios de teste de invasão.

5. O item 3.2.5 do Documento de Oficialização da Demanda conflita com a informação constante do item 2.9 do Anexo do mencionado documento. Faz-se necessário compatibilizar tais informações.

6. O tópico 3 do anexo do Documento de Oficialização da Demanda indica informações a serem prestadas como condição de habilitação de empresa em procedimento licitatório. Tratando-se de procedimento de contratação por Dispensa de Licitação, sugerimos que a área verifique, no caso concreto, se a empresa selecionada já atende àqueles critérios, anexando as respectivas comprovações no procedimento e revisando a redação do tópico de modo a indicar que aquelas características já se encontram comprovada no procedimento.

7. Considerando que as informações constantes no tópico 4 do anexo do Documento de Oficialização da Demanda já constam no item 3.9 do referido documento, sugerimos que o tópico do anexo seja excluído. Ademais, sugerimos a adequação da redação do item 3.9, de modo a indicar que a obrigação da contratada é de assinar o Termo de Confidencialidade e que este documento deverá conter as informações ali dispostas.

Informações não encontradas no DOD, porém constantes na contratação anteriormente realizada:

8. **Relativamente ao recebimento e/ou condição de pagamento (Itens 3.4 e 3.6)**: "A entrega do Relatório de testes é indispensável ao recebimento do objeto deste instrumento, nos termos definidos neste instrumento". Neste sentido, sugerimos tal previsão até mesmo para viabilizar a entrega do último relatório ao recebimento dos serviços executados (e consequentemente melhor documentar a habilitação para pagamento do fornecedor).

9. **Relativamente às obrigações da Contratada (Item 3.9)**: "Acompanhar e informar sobre as atualizações tecnológicas necessárias para executar os serviços adquiridos, realizando as ações necessárias para a implantação dessas atualizações em comum acordo com o **CONTRATANTE**, até o final do contrato, sem ônus para o **CONTRATANTE"**.

Sugestões de melhoria:

10. Sugerimos adequar a redação do item 2.6 do anexo do DOD de modo a evidenciar que as atividades da contratada deverão compreender o conjunto de atividades informado, além de excluir a expressão "DOCUMENTO DE OFICIALIZAÇÃO DA DEMANDA SERVIÇOS DISPENSA" no final do texto. Propomos a seguinte redação (a ser analisada em sua conformidade pela Unidade demandante): "*A **CONTRATADA** deverá desenvolver atividades que, minimamente, busquem encontrar vulnerabilidades em potencial, de eventual má configuração, de falhas em hardwares e softwares desconhecidos, de técnicas de contramedidas ou deficiências na infraestrutura ou sistemas do **CONTRATANTE".***

Por fim, informamos que a minuta do contrato se encontra em fase avançada, dependendo exclusivamente do saneamento destas inconformidades para

ser submetida à aprovação da unidade solicitante.

Após, retorne-se o expediente a esta Unidade.



Documento assinado eletronicamente por **Mariana Nascimento Sotero Campos** em 12/08/2021, às 11:35, conforme art. 1º, III, "b", da Lei 11.419/2006.



A autenticidade do documento pode ser conferida no site https://sei.sistemas.mpba.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0172752** e o código CRC **C251A289**.

EC-Council

Certification Number
ECC8904172635

C|EH Certified Ethical Hacker

Certified Ethical Hacker

This is to acknowledge that

Diogenes Ramos

has successfully completed all requirements and criteria for

Certified Ethical Hacker

certification through examination administered by EC-Council

Issue Date: **21 December, 2020**

Expiry Date: **20 December, 2023**

ANSI ACCREDITED
#0732
ISO/IEC 17024
Personnel Certification Program



Sanjay Bavisi, President

Lloyd's Register

Data de Emissão Atual:	04 de Janeiro de 2021	Aprovações Originais:
Data de validade:	21 de Outubro de 2023	ISO/IEC 27001 - 04 de Janeiro de 2021
Número de Identidade do Certificado:	10343093	

CERTIFICADO DE APROVAÇÃO

Certificamos que o Sistema de Gestão de:

Stefanini Consultoria e Assessoria em Informática S/A

AV. Jaguary 164, Centro, Jaguariúna, 013910-039, São Paulo, Brasil

foi aprovado pelo Lloyd's Register de acordo com a (s) seguinte (s) norma (s):

ISO/IEC 27001:2013

Números de Aprovação: ISO/IEC 27001 – 00028093

Este certificado é válido somente se associado com o anexo do certificado contendo o mesmo número, no qual estão listados os locais aplicáveis a esta aprovação

O escopo de aprovação é aplicável a:
ISO/IEC 27001:2013
Gestão da segurança da informação nas seguintes áreas, proteção das informações proprietárias de clientes externos mantidas nos servidores e datacenters da Stefanini de acordo com a declaração de aplicabilidade Rev. 6.0, Ago 4, 2020.

This certificate is a continuation of a previous approval from another certification body as follows:

Previous original ISO/IEC 27001 approval on 22-OCT-2017, BSI certificate number IS618883

Cliff Muckleroy

Area Operations Manager Americas

Emitido por: Lloyd's Register do Brasil Ltda

Por e em nome de: Lloyd's Register Quality Assurance Limited

UKAS MANAGEMENT SYSTEMS
001

Lloyd's Register Group Limited, its affiliates and subsidiaries, including Lloyd's Register Quality Assurance Limited (LRQA), and their respective officers, employees or agents are, individually and collectively, referred to in this clause as 'Lloyd's Register'. Lloyd's Register assumes no responsibility and shall not be liable to any person for any loss, damage or expense caused by reliance on the information or advice in this document or howsoever provided, unless that person has signed a contract with the relevant Lloyd's Register entity for the provision of this information or advice and in that case any responsibility or liability is exclusively on the terms and conditions set out in that contract. Issued by: Lloyd's Register do Brasil Ltda, Rua Helena, 235 - 11º andar, Vila Olimpia, São Paulo/SP 04552-050, Brasil for and on behalf of: Lloyd's Register Quality Assurance Limited, 1 Trinity Park, Bickenhill Lane, Birmingham B37 7ES, United Kingdom

Anexo Certificação solicitada 2 (0180196) SEI 19.09.02684.0011790/2021-22 / pg. 198

Anexo do Certificado

Localização	Atividades
Stefanini Consultoria e Assessoria em Informática S.A. AV. Jaguary 164, Centro, Jaguariúna, 013910-039, São Paulo, Brasil	**ISO/IEC 27001:2013** Gestão da segurança da informação nas seguintes áreas, proteção das informações proprietárias de clientes externos mantidas nos servidores e datacenters da Stefanini de acordo com a declaração de aplicabilidade Rev. 6.0, Ago 4, 2020.
Stefanini Consultoria e Assessoria em Informática S.A. Rua Alfredo Pujol, 506, Santana, São Paulo, 02017-001, SP, Brasil	**ISO/IEC 27001:2013** Serviços de infraestrutura: gerenciamento de rede, gerenciamento de dados, suporte técnico e "help desk" ("service desk"). Venda de serviços de infraestrutura: gerenciamento de rede, gerenciamento de dados, suporte técnico e "help desk" ("service desk").
Informática & Tecnología Stefanini SA. Calle 122 N°23 - 46, Piso 5 y piso 6, 110111 Bogotá, Colômbia	**ISO/IEC 27001:2013** Desenvolvimento de Software Customizado, Suporte e Manutenção de Aplicativos, Teste de Software, Suporte de Infraestrutura Tecnológica, Fornecimento de Pessoal Especializado e o desenvolvimento e implantação de Sistemas de Informação.
Stefanini India Private Limited. Mahaveer Techno Park (SEEC), Building Plot No. 6 Survey, No 64 4th floor, Software Units Layout Hitec City, Madhapur, 500081, Hyderabad, Índia	**ISO/IEC 27001:2013** Soluções especializadas para ERP, CRM, BI, Desenvolvimento de Aplicações e Serviços Gerenciados (Non-ERP).
Stefanini India Private Limited. C 25, Stellar IT Park, Ground Floor, Tower 1, Sector 62, Uttar Pradesh, Noida, 201307, Índia	**ISO/IEC 27001:2013** Serviços gerenciados de Outsourcing de Tecnologia da Informação.

UKAS MANAGEMENT SYSTEMS
001

Lloyd's Register Group Limited, its affiliates and subsidiaries, including Lloyd's Register Quality Assurance Limited (LRQA), and their respective officers, employees or agents are, individually and collectively, referred to in this clause as 'Lloyd's Register'. Lloyd's Register assumes no responsibility and shall not be liable to any person for any loss, damage or expense caused by reliance on the information or advice in this document or howsoever provided, unless that person has signed a contract with the relevant Lloyd's Register entity for the provision of this information or advice and in that case any responsibility or liability is exclusively on the terms and conditions set out in that contract.
Issued by: Lloyd's Register do Brasil Ltda, Rua Helena, 235 - 11º andar, Vila Olimpia, São Paulo/SP 04552-050, Brasil for and on behalf of: Lloyd's Register Quality Assurance Limited, 1 Trinity Park, Bickenhill Lane, Birmingham B37 7ES, United Kingdom

Anexo Certificação solicitada 2 (0180196) SEI 19.09.02684.0011790/2021-22 / pg. 199

Anexo do Certificado

Localização	Atividades
Stefanini Mexico SA de CV. Blvd. Miguel de Cervantes Saavedra 193, Piso 9 Interior 902, Granada, Miguel Hidalgo, 11520 Ciudad de Mexico, México	**ISO/IEC 27001:2013** Desenvolvimento de Software Customizado, Suporte e Manutenção de Aplicativos, Teste de Software, Suporte de Infraestrutura Tecnológica, Fornecimento de Pessoal Especializado e o desenvolvimento e implantação de Sistemas de Informação, Help Desk (mesa de serviços).
Stefanini Mol SRL Sfatul Țării Street 29, 4th, 6th floors, LeRoy Business Center, MD-2012 Chisinau, Moldávia	**ISO/IEC 27001:2013** Infraestrutura de Tecnologia da Informação (TI) e serviços gerenciados de terceirização de processos de negócios.
Stefanini Philippines, Inc. iMet BPO Tower 1, Metropolitan Park, Macapagal Blvd Corner EDSA, Ext 3rd 5th 6th floors, 1300 Pasay City, Filipinas	**ISO/IEC 27001:2013** Serviços gerenciados de Outsourcing de Tecnologia da Informação e Processos de Negócios.
Stefanini Romania SRL George Constantinescu Street No. 2-4, Global Worth Building 1,2,3, floors Sector 2, 20339 Bucharest, Romênia	**ISO/IEC 27001:2013** Infraestrutura de Tecnologia da Informação (TI) e serviços gerenciados de terceirização de processos de negócios.
Stefanini Romania SRL Calea Dumbrăvii 24 - floors 1-2-3-4-5, 550324 Sibiu, Romênia	**ISO/IEC 27001:2013** Infraestrutura de Tecnologia da Informação (TI) e serviços gerenciados de terceirização de processos de negócios.
Stefanini, Inc. (USA) 27100 West 11 Mile Road, FL 1 5 6 7, Southfield, MI, 48034, Estados Unidos	**ISO/IEC 27001:2013** Serviços gerenciados de Outsourcing de Tecnologia da Informação e Processos de Negócios.

UKAS MANAGEMENT SYSTEMS
001

Lloyd's Register Group Limited, its affiliates and subsidiaries, including Lloyd's Register Quality Assurance Limited (LRQA), and their respective officers, employees or agents are, individually and collectively, referred to in this clause as 'Lloyd's Register'. Lloyd's Register assumes no responsibility and shall not be liable to any person for any loss, damage or expense caused by reliance on the information or advice in this document or howsoever provided, unless that person has signed a contract with the relevant Lloyd's Register entity for the provision of this information or advice and in that case any responsibility or liability is exclusively on the terms and conditions set out in that contract.
Issued by: Lloyd's Register do Brasil Ltda, Rua Helena, 235 - 11º andar, Vila Olimpia, São Paulo/SP 04552-050, Brasil for and on behalf of: Lloyd's Register Quality Assurance Limited, 1 Trinity Park, Bickenhill Lane, Birmingham B37 7ES, United Kingdom

Número de Identidade do Certificado: 10343093

Anexo do Certificado

Localização	Atividades
Top Systems S.A. Pasaje Paseo de las Carretas 2580, floors 1-8, 11300, Montevideo, Uruguai	**ISO/IEC 27001:2013** Comercialização, desenvolvimento, implantação, manutenção e suporte de soluções de TI para instituições financeiras nacionais e internacionais.

UKAS MANAGEMENT SYSTEMS
001

Lloyd's Register Group Limited, its affiliates and subsidiaries, including Lloyd's Register Quality Assurance Limited (LRQA), and their respective officers, employees or agents are, individually and collectively, referred to in this clause as 'Lloyd's Register'. Lloyd's Register assumes no responsibility and shall not be liable to any person for any loss, damage or expense caused by reliance on the information or advice in this document or howsoever provided, unless that person has signed a contract with the relevant Lloyd's Register entity for the provision of this information or advice and in that case any responsibility or liability is exclusively on the terms and conditions set out in that contract.
Issued by: Lloyd's Register do Brasil Ltda, Rua Helena, 235 - 11º andar, Vila Olimpia, São Paulo/SP 04552-050, Brasil for and on behalf of: Lloyd's Register Quality Assurance Limited, 1 Trinity Park, Bickenhill Lane, Birmingham B37 7ES, United Kingdom

Anexo Certificação solicitada 2 (0180196) SEI 19.09.02684.0011790/2021-22 / pg. 201

Jaguariúna, 29 de maio de 2020

DECLARAÇÃO DE COMPROVAÇÃO VÍNCULO EMPRESARIAL

A **STEFANINI CONSULTORIA E ASSESSORIA EM INFORMÁTICA S/A ("STEFANINI")**, sociedade empresária anônima, com sede na cidade de Jaguariúna/SP, à Av. Jaguary, nº 164, Centro, devidamente inscrita no CNPJ sob o nº 58.069.360/0001-20, e **STEFANINI RAFAEL SEGURANÇA E DEFESA S.A. ("STEFANINI RAFAEL")**, sociedade empresária anônima, devidamente inscrita no CNPJ sob o nº 24.691.488/0001-09, com sede à Av. Eusébio Matoso, 1375, 8º andar, sala 801e 802, Butantã - SP, CEP: 05.423-905, São Paulo/SP, por meio desta **DECLARAM** que, fazem parte do mesmo grupo econômico, conforme documentos societários anexos, vide organograma abaixo:



Atenciosamente,

MARIA MAGALI BREDARIOL [redacted]
Assinado de forma digital por MARIA MAGALI [redacted]
Dados: 2020.05.29 15:03:34 -03'00'

STEFANINI CONSULTORIA E ASSESSORIA EM INFORMÁTICA S/A ("STEFANINI")

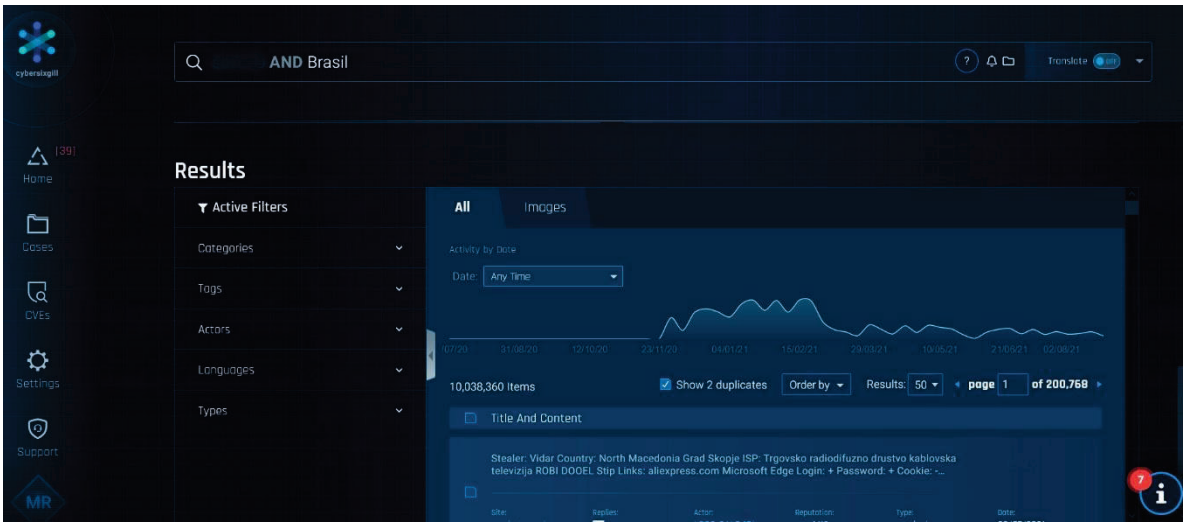
MARIA MAGALI BREDARIOL [redacted]
-03'00'

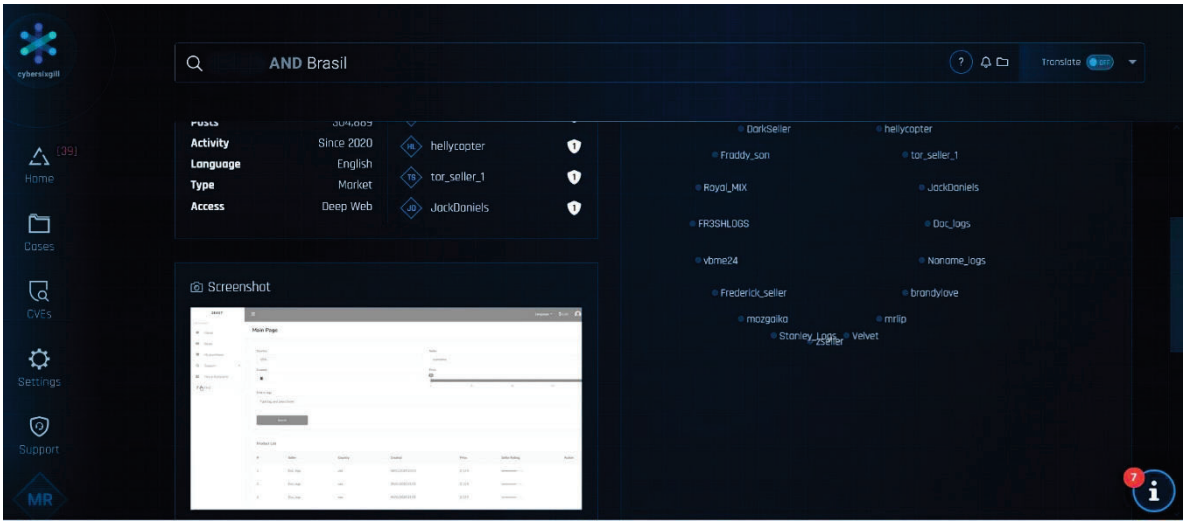
STEFANINI RAFAEL SEGURANÇA E DEFESA S.A. ("STEFANINI RAFAEL")

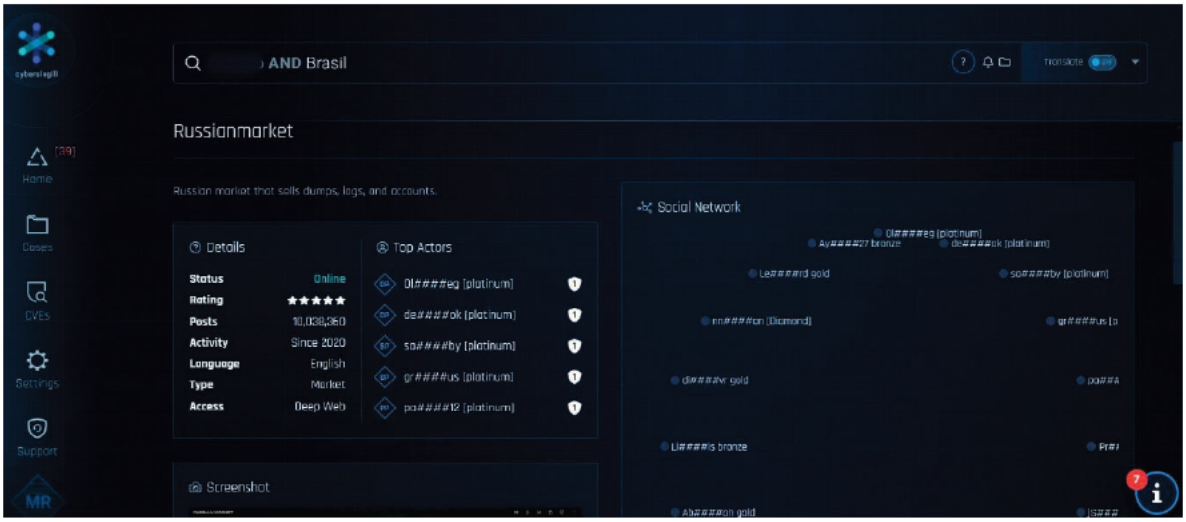
DECLARAÇÃO

STEFANINI RAFAEL SEGURANÇA E DEFESA S.A., com sede na cidade de São Paulo, Estado de São Paulo, na Av. Eusébio Matoso, 1375, 8º andar, sala 801 e 802, Butantã CEP: 05.423-905, inscrito no CNPJ/MF sob o nº 24.691.488/0001-09, de acordo com o solicitado no documento Especificação Técnica MP BA - Pentest Voto Eletrônico, declara para os devidos fins que possui em sua estrutura, produtos de software para pesquisa e análise em Surface Web, Deep Web e Dark Web.

Anexamos a seguir telas de um destes produtos, que auxiliam nas atividades e no conhecimento de inteligência de ameaças cibernéticas (Threat Intelligence).







São Paulo, 17 de agosto de 2021.

MARIA MAGALI BREDARIOL [redacted]

STEFANINI RAFAEL SEGURANÇA E DEFESA S.A.
Maria Magali Bredariol - Diretora Jurídica
CPF/MF nº 437.349.448-72

Testemunhas:

LUIZ CARLOS MARQUES DE AGUIAR [redacted]

Nome: Luiz Carlos Marques De Aguiar
CPF: [redacted]

RAFAEL ALVES PINTO Assinado de forma digital por RAFAEL ALVES PINTO Dados: 2021.08.17 15:31:01 -03'00'

Nome: Rafael Alves Pinto
CPF: [redacted]

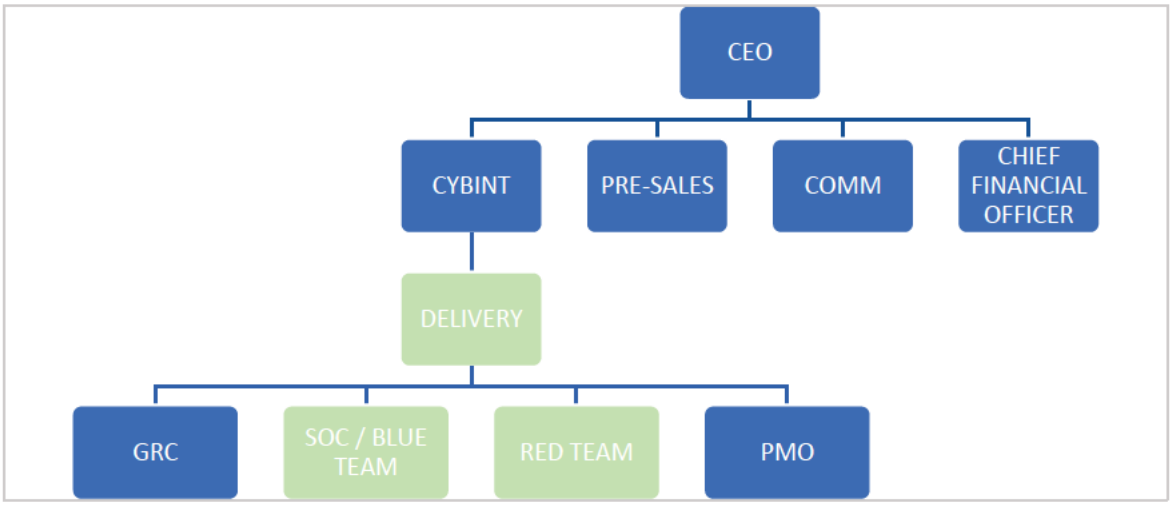
stefaninirafael

DECLARAÇÃO

STEFANINI RAFAEL SEGURANÇA E DEFESA S.A., com sede na cidade de São Paulo, Estado de São Paulo, na Av. Eusébio Matoso, 1375, 8º andar, sala 801 e 802, Butantã CEP: 05.423-905, inscrito no CNPJ/MF sob o nº 24.691.488/0001-09, de acordo com o solicitado no documento Especificação Técnica MP BA - Pentest Voto Eletrônico, declara para os devidos fins que possui em sua estrutura, as equipes de BLUE TEAM e RED TEAM.

Estas equipes realizam Serviços Gerenciados de Segurança (Managed Security Services – MSS) e possuem experiência na execução de serviços similares.

A seguir apresentamos o organograma macro da empresa, visando demonstrar a posição destas equipes dentro de nossa estrutura.



São Paulo, 17 de agosto de 2021.

MARIA MAGALI BREDARIOL [redacted]

STEFANINI RAFAEL SEGURANÇA E DEFESA S.A.
Maria Magali Bredariol - Diretora Jurídica
CPF/MF n [redacted]

Testemunhas:

LUIZ CARLOS MARQUES DE AGUIAR [redacted]0

Nome: Luiz Carlos Marques De Aguiar

CPF: [redacted]

RAFAEL ALVES PINTO Assinado de forma digital por RAFAEL ALVES PINTO Dados: 2021.08.17 15:29:39 -03'00'

Nome: Rafael Alves Pinto

CPF: [redacted]

DECLARAÇÃO

STEFANINI RAFAEL SEGURANÇA E DEFESA S.A., com sede na cidade de São Paulo, Estado de São Paulo, na Av. Eusébio Matoso, 1375, 8º andar, sala 801 e 802, Butantã CEP: 05.423-905, inscrito no CNPJ/MF sob o nº 24.691.488/0001-09, de acordo com o solicitado no documento Especificação Técnica MP BA - Pentest Voto Eletrônico, declara para os devidos fins que possui os seguintes casos de sucesso de suporte à recuperação de ataques cibernéticos:

Cliente: Sodexo Brasil
Necessidade: O cliente encontrava-se em cenário de constantes ataques cibernéticos e fraudes e necessitava de assessment consultivo para a recuperação de ataques cibernéticos.
Projeto: Reconhecimento do ambiente, identificação das causas principais por meio de Root Cause Analysis e por fim, restabelecimento do ambiente atacado, com medidas protetivas e plano de mitigação de riscos. Projeto desenvolvido com atendimento de operação local com time de entrega de Israel, mas com visibilidade global devido a Sodexo Brasil exercer a liderança na transformação digital global em sua área de atuação.

Cliente: Raizen
Necessidade: O cliente encontrava-se em situação de ataques contínuos e uma solução tradicional de análise contínua de risco e pen test não seriam suficientes.
Projeto: Melhoria na arquitetura de segurança da organização, melhoria na resposta de detecção de ameaças e aumento da resiliência para a recuperação de ataques futuros. Aplicação de tecnologias de origem Israelense e exclusiva no Brasil, com expertise técnico de elite (profissionais com +10 anos de background em cybersecurity).

Cliente: Vallourec
Necessidade: Gestão de Vulnerabilidades, Governança, Riscos e Compliance - Serviços Especializados de Cyber Security (Inteligência)
Projeto: Prover e manter uma estrutura de serviços apta à realização de atividades de Ethical Hacking em aplicações e/ou sistemas, seguindo escalas cíclicas de verificação das soluções, bem como para atendimento a demandas eventuais para novos projetos e/ou demandas específicas. Responsável pela elaboração de relatório gerencial mensal sobre ameaças, ataques e tentativas de invasões ao ambiente computacional da Vallourec.

Anexo Certificação solicitada 6 (0180204) SEI 19.09.02684.0011790/2021-22 / pg. 207

São Paulo, 17 de agosto de 2021.

MARIA MAGALI BREDARIOL [redacted]

STEFANINI RAFAEL SEGURANÇA E DEFESA S.A.
Maria Magali Bredariol - Diretora Jurídica
CPF/MF nº [redacted]

Testemunhas:

LUIZ CARLOS MARQUES DE AGUIAR [redacted]

Nome: Luiz Carlos Marques De Aguiar
CPF: [redacted]

RAFAEL ALVES PINTO

Nome: Rafael Alves Pinto
CPF: [redacted]

stefaninirafael

DECLARAÇÃO

STEFANINI RAFAEL SEGURANÇA E DEFESA S.A., com sede na cidade de São Paulo, Estado de São Paulo, na Av. Eusébio Matoso, 1375, 8º andar, sala 801 e 802, Butantã CEP: 05.423-905, inscrito no CNPJ/MF sob o nº 24.691.488/0001-09, de acordo com o solicitado no documento Especificação Técnica MP BA - Pentest Voto Eletrônico, declara para os devidos fins que possui mais de três anos de funcionamento, conforme comprovante de inscrição e de situação cadastral emitido pelo Cadastro Nacional de Pessoa Jurídica (CNPJ), anexo a esta declaração.

São Paulo, 17 de agosto de 2021.

MARIA MAGALI BREDARIOL [redacted]

STEFANINI RAFAEL SEGURANÇA E DEFESA S.A.
Maria Magali Bredariol - Diretora Jurídica
CPF/MF nº [redacted]

Testemunhas:

LUIZ CARLOS MARQUES DE [redacted]

Nome: Luiz Carlos Marques De Aguiar
CPF: [redacted]

RAFAEL ALVES PINTO Assinado de forma digital por RAFAEL ALVES PINTO Dados: 2021.08.17 15:32:25 -03'00'

Nome: Rafael Alves Pinto
CPF: [redacted]

REPÚBLICA FEDERATIVA DO BRASIL

CADASTRO NACIONAL DA PESSOA JURÍDICA

NÚMERO DE INSCRIÇÃO	COMPROVANTE DE INSCRIÇÃO E DE SITUAÇÃO CADASTRAL	DATA DE ABERTURA
24.691.488/0001-09 MATRIZ		29/04/2016

NOME EMPRESARIAL
STEFANINI RAFAEL SEGURANCA E DEFESA S.A.

TÍTULO DO ESTABELECIMENTO (NOME DE FANTASIA)	PORTE
********	DEMAIS

CÓDIGO E DESCRIÇÃO DA ATIVIDADE ECONÔMICA PRINCIPAL
62.03-1-00 - Desenvolvimento e licenciamento de programas de computador não-customizáveis

CÓDIGO E DESCRIÇÃO DAS ATIVIDADES ECONÔMICAS SECUNDÁRIAS
46.51-6-01 - Comércio atacadista de equipamentos de informática
62.01-5-01 - Desenvolvimento de programas de computador sob encomenda
62.02-3-00 - Desenvolvimento e licenciamento de programas de computador customizáveis
62.04-0-00 - Consultoria em tecnologia da informação
62.09-1-00 - Suporte técnico, manutenção e outros serviços em tecnologia da informação
63.19-4-00 - Portais, provedores de conteúdo e outros serviços de informação na internet
64.62-0-00 - Holdings de instituições não-financeiras
95.11-8-00 - Reparação e manutenção de computadores e de equipamentos periféricos

CÓDIGO E DESCRIÇÃO DA NATUREZA JURÍDICA
205-4 - Sociedade Anônima Fechada

LOGRADOURO	NÚMERO	COMPLEMENTO
AV EUSEBIO MATOSO 1375	1375	ANDAR 8 SALA 801 E 802

CEP	BAIRRO/DISTRITO	MUNICÍPIO	UF
05.423-905	BUTANTA	SAO PAULO	SP

ENDEREÇO ELETRÔNICO	TELEFONE
GESTAOTRIBUTARIA@STEFANINI.COM	(11) 3094-6174

ENTE FEDERATIVO RESPONSÁVEL (EFR)
*****

SITUAÇÃO CADASTRAL	DATA DA SITUAÇÃO CADASTRAL
ATIVA	29/04/2016

MOTIVO DE SITUAÇÃO CADASTRAL

SITUAÇÃO ESPECIAL	DATA DA SITUAÇÃO ESPECIAL
********	********

Aprovado pela Instrução Normativa RFB nº 1.863, de 27 de dezembro de 2018.

Emitido no dia **16/08/2021** às **11:22:08** (data e hora de Brasília). Página: **1/1**

Anexo Certificação solicitada 8 (0180206) SEI 19.09.02684.0011790/2021-22 / pg. 210

hapvida

ATESTADO DE PRESTAÇÃO DE SERVIÇOS

Atestamos para os devidos fins que a empresa STEFANINI RAFAEL SEGURANCA E DEFESA S.A. , inscrita no CNPJ 24.691.488/0001-09, estabelecida em AV EUSEBIO MATOSO 1375, ANDAR 8 SALA 801 E 802, CEP 05.423-905, BUTANTA SP, prestou serviços na área de Segurança da Informação dentro dos níveis de serviços contratados, conforme projeto descrito abaixo :

O projeto desenvolvido pela Contratada possuia os seguintes objetivos:

- Estruturar a area de Segurança de Informação;
- Realizar diagnostico da situação atual relativo aos aspectos de segurança da informação na empresa contratante;
- Produzir documentos relacionados ao escopo do projeto; tais como Politica da Segurança de Informação;
- Produzir documentos com caracteristicas de Instruções normativas para atender procedimentos ou processo da area de segurança de informação; a exemplo de Backup e restore, gerenciamento de acesso dentre outros.
- Produzir documentos com recomendações para que possam ser criados planos de ações para crescimento e adequação da area de segurança da informação

1. Metodologia de desenvolvimento do projeto
   O projeto foi desenvolvimento com a metodologia de gestão de projeto baseado nas boas praticas de PMI - Project Managment Institute. As reuniões de status report semanais garantia a boa comunicação e acompanhamento do projeto.

2. Recursos alocados ao projeto
   Os recursos humanos do projeto atendia as expectativas exigidas pela empresa contratante com dedicação exclusiva ao desenvolvimento do projeto.

3. Porte do projeto
   Projeto desenvolvido em 1.296 hs, com entregas parciais.

Declaramos, ainda, que a mesma demostra capacidade técnica e de gestão dentro dos níveis de serviços contratdos, cumprindo com qualidade os termos do contrato firmado e nada constando em seu desabono até a presente data.

Informações da Empresa cliente e responsável
Empresa: HAPVIDA ASSISTENCIA MEDICA LTDA , CNPJ 63.554.067/0001-98
Endereço: AV. HERACLITO GRACA, 406 - 2º ANDAR FORTALEZA -CE
Responsável: Bruno Cascão Lima
Cargo: Gerente Segurança da Informação
E-mail: brunol@hapvida.com.br
Telefone: 85 99150-6428

Fortaleza, 28 de novembro de 2019

ATESTADO DE CAPACIDADE TÉCNICA

Atestamos, para os devidos fins orientados para relações comercias entre partes, que a empresa **Stefanini Rafael Segurança e Defesa S.A.**, inscrita no CNPJ/MF n° 24.691.488/0001-09, situada na Avenida Eusébio Matoso, 1375 - 8° andar – Butantã – São Paulo CEP: 05423-905, realiza, para a Vallourec Tubos do Brasil Ltda, inscrita no CNPJ nº 17.170.150/0001-46, estabelecida na Avenida Olinto Meireles, nº 65, bairro Barreiro na cidade de Belo Horizonte, MG, o fornecimento de serviços gerenciados abaixo relacionados, objetos escopo do contrato vigente nº 10002862, obedecendo à qualidade e demais condições técnicas estabelecidas.

Escopo de fornecimento, conforme **Anexo I - Escopo de trabalho - Contrato de Outsourcing de Infraestrutura:**

A. Monitorar e avaliar o desempenho do Contrato

1. Disponibilizar no máximo até 5 dias a partir do 1° dia útil do mês subsequente (5° dia útil) a prestação dos serviços, os seguintes relatórios aplicáveis:
   - Relatório Geral de Riscos, Conformidade para Controles Internos
   - Relatório Geral de Incidentes / Problemas de Segurança da Informação
   - Relatório Geral de Indicadores de Segurança da Informação
   - Relatório Geral de Análise de Vulnerabilidades
   - Relatório Geral de Análise de Ameaças, Prevenção e Detecção de Intrusão

B. Gestão de Vulnerabilidades, Governança, Riscos e Compliance - Serviços Especializados de Cyber Security (Inteligência)

1. Prover e manter uma estrutura de serviços adequada e habilitada à Gestão de Riscos (lógicos e/ou físicos no ambiente da Vallourec) com foco na análise, gerenciamento e aplicação de contramedidas de prevenção, mitigação e ou bloqueio de ameaças e/ou deficiências de controles internos, que, se exploradas , possam vir a causar impactos e/ou danos às operações de negócios da Vallourec.
2. Manter, aplicar e controlar as políticas de Segurança da Informação estabelecidas entre as partes através do Manual de Segurança da Informação da Segurança, instrumento este, componente da Política de Segurança da Informação da Vallourec, que direciona as definições, controles e regras principais para a operacionalização do processo no ambiente da Vallourec.
3. Prover e manter uma estrutura de serviços adequada a realizar o processo contínuo de Análise de Vulnerabilidades nos ambientes, sistemas, aplicações e serviços de processamento de dados da Vallourec, como controle interno preventivo fundamental e parte da Gestão de Riscos acima referenciada. Planos de Ações relacionados serão gerenciados em conjunto e entre as partes.
4. Especificamente para aplicações e/ou sistemas de informação, prover e manter uma estrutura de serviços apta à realização de atividades de *Ethical Hacking* em aplicações e/ou sistemas, seguindo escalas cíclicas de verificação das soluções, bem como para atendimento a demandas eventuais para novos projetos e/ou demandas específicas.
5. Gerenciar as recomendações de correções de segurança para todo o ambiente computacional da Vallourec, seguindo, inclusive, os prazos máximos de mitigação acordados entre as partes e estabelecidos no Manual de Segurança da Informação.

6. Prover e manter uma estrutura de serviços adequada de respostas às novas ameaças identificadas e classificadas pelos principais *Security Response Teams* mundiais, o que inclui o gerenciamento da aplicação de correções ou contramedidas em caráter emergencial.
7. Prover e manter uma estrutura de serviços adequada e habilitada ao monitoramento e resposta, em regime 24hx7x365 (Security Operation Center - SOC), de incidentes de Segurança da Informação nos ambientes computacionais da Vallourec, através de correlacionamento de logs, eventos, tráfegos e pacotes de redes, e/ou comportamento não esperado de aplicações e/ou serviços, dentre outros. Total de ativos monitorados 4872 (*Assets*).
8. Prover e manter uma estrutura de serviços qualificada e habilitada para registrar, analisar, classificar, remediar, responder e documentar os incidentes de Segurança da Informação gerados por ambas as partes, para toda a vigência do contrato, incluindo a rastreabilidade e auditabilidade necessárias.
9. Responsável pelas respostas e tratativas relacionadas aos incidentes e/ou riscos registrados a partir da plataforma integrada de SIEM, *HoneyPot* e *EndPoint Protection* provida Vallourec, doravante denominada eGambit (by Tehtris).
10. Prover e manter uma estrutura de serviços e equipe qualificada para atendimento especializado para resposta e/ou investigação de incidentes críticos envolvendo a estrutura computacional da Vallourec, incluído aspectos e/ou requerimentos de Análises Forenses.
11. Responsável por atender quaisquer demandas de controles internos associados à Tecnologia da Informação da Vallourec para atendimento às suas exigências legais de *compliance* e de auditorias internas e externas, incluindo todo o levantamento e evidenciamento sempre que solicitados com ou sem aviso prévio da Vallourec e sem nenhum tipo de restrição de acesso as informações ora solicitadas.
12. Prover e manter uma capacidade de suporte técnico consultivo para a Segurança da Informação da Vallourec sobre questões relativas ao processo, suas soluções, recursos e/ou contramedidas aplicáveis.
13. Responsável por aplicar as políticas do Manual de Segurança da Informação da Vallourec, instrumento este que direcionará as definições, controles e regras principais para a operacionalização do processo de Segurança da Informação no ambiente da Vallourec.
14. Responsável por participar e atuar nas reuniões mensais de Gerenciamento de Segurança da Informação da Vallourec, respondendo ao acompanhamento e gerenciamento de planos de ações e/ou de incidentes relacionados.
15. Prover e manter uma estrutura mensal apta à publicação, análise e gerenciamento dos relatórios e entregáveis de gestão dos serviços, apuração de resultados de SLAs e gestão do processo junto à Vallourec e à OPERAÇÃO do ambiente.
16. Responsável pela elaboração de relatório gerencial mensal sobre ameaças, ataques e tentativas de invasões ao ambiente computacional da Vallourec.

O fornecimento está sendo realizado desde Junho de 2019, atendendo às finalidades a que foi destinado, não havendo até a presente data nenhum fato que desabone o fornecedor técnica e comercialmente.

Belo Horizonte, 06 de Agosto de 2021.

Assinado de forma digital
por SABRINA SILVEIRA
BORBA[redacted]

Sabrina Borba

INFORMATION SECURITY POLICY

Information Security Management System



Code:	ISMS-001
Version:	1.1
Date of version:	11-AUG-2015
Created by:	Matthew Engler
Approved by:	Washington Souza
Confidentiality level:	Internal Use

Table of contents

1. PURPOSE, SCOPE AND USERS 3

1.1. BASIC INFORMATION SECURITY TERMINOLOGY 3

2. REFERENCE DOCUMENTS 3

3. DESCRIPTION 3

3.1. MANAGING THE INFORMATION SECURITY 3

3.1.1. Objectives and measurement 4

3.1.2. Information security requirements 4

3.1.3. Information security controls 4

3.1.4. Business continuity 4

3.1.5. Responsibilities 4

3.1.6. Policy communication 5

3.2. SUPPORT FOR ISMS IMPLEMENTATION 5

4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 5

5. DOCUMENT MANAGEMENT 5

6. APPENDICES 6

7. CHANGE HISTORY 6

APPENDICE 1 6

INFORMATION SECURITY POLICY (EXTERNAL COMMUNICATION) 6

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 215

1. Purpose, scope and users

The aim of this top-level Policy is to define the purpose, direction, principles and basic rules for information security management.

This policy applies to Stefanini Employees, sub-contractors, consultants, business associates, and other workers at Stefanini (collectively "User(s)")

1.1. Basic Information Security Terminology

Confidentiality – Ensuring information is not made available or disclosed to unauthorized individuals, entities, or processes.

Integrity – Ensuring information is accurate and reliable and has not been subtly changed or tampered with by an unauthorized party. Integrity includes:

- Authenticity: The ability to verify content has not changed in an unauthorized manner.
- Non-repudiation & Accountability: The origin of any action on the system can be verified and associated with a user.

Availability – Ensuring timely and reliable access to and use of information by authorized persons. Information is unavailable not only when it is lost or destroyed, but also when access to the information is denied or delayed to an authorized person.

Information Security – Preservation of confidentiality, integrity and availability of information.

Information Security Management System – Part of overall management processes that take care of planning, implementing, maintaining, reviewing, and improving the information security.

2. Reference documents

Documents associated or linked are listed below:

- ISO/IEC 27001 standard, clauses 5.2 and 5.3
- ISMS-002 Manual, Information Security Management System
- ISMS-003 Statement of Applicability
- ISMS-005 Procedure, Identification of requirements
- ISMS-019 Procedure, Risk Analysis
- ISMS-020 Procedure, Risk Treatment Plan
- ISMS-023 Procedure, Incident Management
- ISMS-031 Policy, Business Continuity Management
- ISMS-034 List of Legal, Regulatory and other requirements

3. Description

3.1. Managing the Information Security

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 216

3.1.1. Objectives and measurement

General objectives for the information security management system are the following: creating a better market image and reducing the damage caused by potential incidents; goals are in line with the organization's business objectives, strategy and business plans.
The Top Management / Top Management Representative, together with the support of the Information Security Manager and Security Committee are responsible for reviewing these general ISMS objectives and setting new ones.

Objectives for individual security controls or groups of controls are proposed by the Security Committee and approved by the Information Security Manager in the Statement of Applicability.

All the objectives must be reviewed at least once a year.

Stefanini will measure the fulfillment of all the objectives. The Top Management Representative is responsible for setting the method for measuring the achievement of the objectives – the measurement will be performed at least once a year and the Information Security Manager will analyze and evaluate the measurement results and report them to the Top Management Representative as input materials for the Management review.

3.1.2. Information security requirements

This Policy and the entire ISMS must be compliant with legal and regulatory requirements relevant to the organization in the field of information security, as well as with contractual obligations.

A detailed list of all legal or regulatory requirements is provided in the ISMS-034 List of Legal, Regulatory and other requirements.

3.1.3. Information security controls

The processes of selecting the controls (safeguards) are defined in the ISMS-019 Procedure, Risk Analysis and ISMS-020 Procedure, Risk Treatment Plan.

The selected controls and their implementation status are listed in the ISMS-003 Statement of Applicability.

3.1.4. Business continuity

Business continuity management is prescribed in the ISMS-031 Business Continuity Management Policy.

3.1.5. Responsibilities

Responsibilities for the ISMS are the following:

- Top Management Representative is responsible for ensuring that the ISMS is implemented and maintained according to this Policy, and for ensuring all necessary resources are available
- Information Security Manager is responsible for operational coordination of the ISMS as well as for reporting about the performance of the ISMS
- Top Management must review the ISMS at least once a year or each time a significant change occurs, and prepare minutes from that meeting. The purpose of the management review is to establish the suitability, adequacy and effectiveness of the ISMS.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 217

- The Human Resources department, together with the support of the Information Security Manager is responsible for adopting and implementing the Training and Awareness Plan, which applies to all persons who have a role in information security management system
- The protection of integrity, availability, and confidentiality of assets is accountable to the owner of each asset
- All security incidents or weaknesses must be reported to Information Security Manager
- The Information Security Manager will define which information related to information security will be communicated to which interested party (both internal and external), by whom and when

3.1.6. Policy communication

The Human Resources department, together with the support of the Information Security Manager has to ensure that all employees of Stefanini, as well as appropriate external parties are familiar with this Policy.

To communicate the policy externally, a summarized version of the policy, found in Appendix 1, will be published on websites, agreements or for commercial purposes, where appropriate. Where a properly executed confidentiality agreement exists, the Information Security Policy in its entirety will be provided.

3.2. Support for ISMS implementation

Hereby the Top Management declares that ISMS implementation and continual improvement will be supported with adequate resources in order to achieve all objectives set in this Policy, as well as satisfy all identified requirements.

4. Managing records kept on the basis of this document

- Not applicable

5. Document management

The owner of this document is the Top Management Representative, who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria must be considered:

- number of employees and external parties who have a role in the ISMS, but are not familiar with this document
- non-compliance of the ISMS with the laws and regulations, contractual obligations, and other internal documents of the organization
- ineffectiveness of ISMS implementation and maintenance
- unclear responsibilities for ISMS implementation

A current version of this document is available to all staff and under version control on the corporate document control system.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 218

6. Appendices

- Appendice 1 : Information Security Policy (external communication).

7. Change history

Date	Version	Created by	Description of change
11-DEC-2013	1.0	Rodrigo Ricci	Document creation
11-AUG-2015	1.1	Matthew Engler	Updated definitions of C, I, A; Assigned measurement responsibilities to Info Sec Manager.

Appendice 1

Information Security Policy (external communication)

The Top Management of Stefanini recognizes the importance of identifying and protecting the information assets of the organization, avoiding destruction, improper disclosure, improper modification or unauthorized use of any information relating to its customers, employees, pricing, strategy, management, or other related concepts.

Stefanini is therefore committed to develop, implement, maintain and continually improve the Information Security Management System (ISMS) in order to ensure the confidentiality, availability and integrity of information.

To achieve this goal, Stefanini:

- Establishes annual objectives in relation to Information Security.
- Ensures the identification and fulfillment of business requirements, contractual, legal and regulatory obligations of security.
- Develops a process of risk analysis, and, according to its results, implements the appropriate actions in order to address risks that are deemed unacceptable based on criteria established in the Risks Identification and Assessment process.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 219

INFORMATION SECURITY MANAGEMENT SYSTEM MANUAL

Information Security Management System



Code:	ISMS-002
Version:	8.0
Date of version:	01-JUL-2020
Updated by:	Elaine Pinheiro
Approved by:	Washington Souza
Confidentiality level:	Internal Use

Table of contents

1. PURPOSE, SCOPE AND USERS 4

2. REFERENCE DOCUMENTS 4

3. ISMS STRUCTURE 4

4. CONTEXT OF THE ORGANIZATION 4

4.1. UNDERSTANDING THE ORGANIZATION AND ITS CONTEXT 4

4.2. UNDERSTANDING THE NEEDS AND EXPECTATIONS OF INTERESTED PARTIES 7

4.3. CERTIFICATION SCOPE FOR ISO 27001:2013 7

4.4. INFORMATION SECURITY MANAGEMENT SYSTEM 7

5. LEADERSHIP 7

5.1. LEADERSHIP AND COMMITMENT 7

5.2. POLICY 8

5.3. ORGANIZATIONAL ROLES, RESPONSIBILITIES AND AUTHORITIES 8

6. PLANNING 8

6.1. ACTIONS TO ADDRESS RISKS AND OPPORTUNITIES 8

6.2. INFORMATION SECURITY OBJECTIVES AND PLANS FOR THEIR ACHIEVEMENT 9

7. SUPPORT 9

7.1. RESOURCES 9

7.2. COMPETENCE 9

7.3. AWARENESS 10

7.4. COMMUNICATION 10

7.5. DOCUMENTED INFORMATION 11

8. OPERATION 11

8.1. OPERATIONAL PLANNING AND CONTROL 11

8.2. INFORMATION SECURITY RISK ASSESSMENT 11

8.3. INFORMATION SECURITY RISK TREATMENT 11

9. PERFORMANCE EVALUATION 12

9.1. MONITORING, MEASUREMENT, ANALYSIS AND EVALUATION 12

9.2. INTERNAL AUDIT 12

9.3. MANAGEMENT REVIEW 12

10. PERFORMANCE EVALUATION 12

10.1. NONCONFORMITY AND CORRECTIVE ACTION 12

10.2. CONTINUAL IMPROVEMENT 12

11. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 13

12. DOCUMENT MANAGEMENT 13

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 221

13. APPENDICES 13

14. CHANGE HISTORY 13

APPENDIX A: SECURITY GOVERNANCE COMMITTEE CHARTER 14

Committee 14

Scope of Topics Considered 14

Charge 14

Membership 15

Meetings 15

Items Requiring Rapid Response 15

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 222

1. Purpose, scope and users

The purpose of this ISMS Manual is to describe how Stefanini established its security management system and addresses the proper policies, procedures and controls that meet the standard requirements.

This manual is applied to all employees and third parties that may affect the Information Security Management System (ISMS).

Users of this document includes Stefanini Employees, sub-contractors, consultants, business associates, and other workers at Stefanini, including all personnel affiliated with third parties and subsidiaries on the Stefanini infrastructure (collectively "User(s)").

2. Reference documents

Documents associated or linked to this one are listed below:

- ISO/IEC 27001 standard, second edition, 01-10-2013.
- ISMS-001 Policy, Information Security
- RACI Chart: Refer to ISO 27001 Document Map Spreadsheet

3. ISMS Structure

The ISMS is structured on **Policies** which outlines specific requirements or rules that must be met in order to mitigate a security risk, **Standards** which are a collection of system-specific or procedural-specific requirements that must be met by everyone in order to comply with a policy, **Procedures** which describe the way to meet the policies´ statements and controls and **Monitoring** for evidence of the policies and standards compliance.

4. Context of the organization

4.1. Understanding the organization and its context

Stefanini determined external and internal risks that are relevant to its purpose and that affects its ability to achieve the intended outcome(s) of its information security management system.

4.1.1. Internal Context

Stefanini operations consist of Service Delivery (help desk support), Application Management Support (AMS), Enterprise Services Support (NOC, Server Administration, SCCM Administration), software deployment and data hosting for our clients. These services are provided at several locations and supported by Stefanini Employees, Stefanini Contracted Staff (Contingent Workers) and Stefanini Support Suppliers. The organization's operations are divided by hemispheres, the Northern Hemisphere and Southern Hemisphere.

The Northern Hemisphere operates Service Delivery out of seven (7) ISO 27001:2013 in-scope locations: Southfield, MI USA; Bucharest, Romania; Sibiu, Romania; Chișinău, Moldova; Manila, Philippines; Noida, India; and Dalian, China. Application Management Support (AMS) operates out of three (3) ISO 27001:2013 in-scope locations: Bucharest, Romania; Chișinău, Moldova; and Hyderabad, India. Enterprise Services Support operates out of three (3) ISO 27001:2013 in-scope locations: Bucharest, Romania; Manila, Philippines; and

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 223

Noida, India. Software deployment is operated out of three in-scope locations, Southfield, MI USA; Bucharest, Romania; and Manila, Philippines. Data hosting is operated out of two outsourced co-locations, Royal Oak, MI USA and Machelen, Belgium. Only data hosted on behalf of a customer delivered from an in-scope location is considered in-scope for the data center. These datacenters also house the main IT equipment used for Service Delivery.

The Southfield, MI USA office is the main headquarters for the Northern Hemisphere operations. Bucharest, Romania houses the tier 0 and tier 1 support for the internal Support desk for Northern Hemisphere.

The Stefanini Mexico CDMX office operates the following commercial services, delivery service: (Development of software applications), AMS (Application support), ATS (Automation and application testing), ITO (Technological infrastructure), call center services, maintenance and support of IT solutions. All these services use the data center that is located in the same building.

The Southern Hemisphere operates Service Delivery and data hosting out of four ISO 27001:2013 in-scope locations: Santana, São Paulo, Brazil; Jaguariuna, São Paulo, Brazil; Bogota, Colombia; and Montevideo, Uruguay. Service Delivery covers the functions of the Service Desk, Software deployment and ICT group who also provide the internal Support desk for Southern Hemisphere operations.

The Jaguariúna, São Paulo, Brazil office is the main headquarters for the ISO 27001:2013. The Jaguariuna, São Paulo, Brazil office counts on Corporatives areas support.

The Calle 122 office in Bogotá, Colombia operates the following delivery services: ADS (Software application development), AMS (Application support), ATS (Automation and application testing), and ITO (Administration, management and support of technological infrastructure for help desk services, callcenter, cloud services), Analytics and Automation, Consulting and Infovisual. All these services use the data center located in the same building.

The Montevideo, Uruguay office operates the following services: marketing, development, implementation, maintenance and support of IT solutions for national and international financial institutions. All these services use the data center that is located in the same facility.

Stefanini supports several different customers from several different commercial interests requiring flexibility in deployment and a broad base of compliance requirements. Stefanini's operations function within a lean model for delivery of services, looking to maximize return on investment through low cost initiatives.

4.1.2. External Context

Stefanini operations are conducted in several locations requiring a strong understanding of local political and environmental concerns. All facilities are subject to standard emergency events such as fire, power failure and HVAC failures.

The Southfield, MI USA facility is located in a shared, multi-story building in Southfield, Michigan. This facility is located within a relatively low risk political and environmental location. This facility is located in an area where severe winter weather can occur resulting in power outages or workers unable to report.

The Bucharest, Romania facility is located on the 1st through 3rd floors of a shared, multi-story building in Bucharest, Romania. This facility is located in a low risk political and medium risk environmental location. This facility is located in an area where earthquakes are possible. In addition, public transit work stoppages could prevent employees from reporting to the facility.

The Sibiu, Romania facility is located on the 1st through 5th floors of a shared, multi-story building in Sibiu, Romania. This facility is located in a low risk political and medium risk environmental location. This facility is located in an area where earthquakes are possible.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 224

The Chișinău, Moldova facility is located on the 4th and 6th floors of a shared, multi-story building in Chișinău, Moldova. This facility is located in a medium-high risk political and medium-high risk environmental location. This facility is located in an area where earthquakes are possible, although only occur years apart. Moldova has political risks surrounding economic stability and the functioning of the government in a transparent and prudent manner.

The Hyderabad, India facility is located on the 4th floor of a shared, multi-story building in Hyderabad, India. This facility is located in a medium-high risk political and medium-high risk environmental location. The region is vulnerable to a wide range of natural hazards, particularly flooding, drought, extreme heat waves, cyclones, landslides and earthquakes. Power outages may be frequent. This could result in loss of power to the facility and difficulties in delivering services. Border tensions with neighbours have been elevated in the past few years.

The Noida, India facility is located on the 5th floor of a shared, multi-story building in Noida, India. This facility is located in a medium-high risk political and medium-high risk environmental location. The region is vulnerable to a wide range of natural hazards, particularly flooding, drought, extreme heat waves, cyclones, landslides and earthquakes. Power outages may be frequent. This could result in loss of power to the facility and difficulties in delivering services. Border tensions with neighbours have been elevated in the past few years.

The Manila, Philippines facility is located on the 3rd through 6th floors of a shared, multi-story building in Pasay, Philippines. This facility is located in a low-medium risk political and medium risk environmental location. This facility has common occurrence of typhoon which may result in flooding around the region. This may prevent workers from getting to the facility or being able to leave the facility.

The Dalian, China facility is located on the 2nd and 4th floors of a shared, multi-story building in Dalian, China. This facility is located in a low risk political and low risk environmental location. Government working restrictions may present difficulty in managing the facility.

The Stefanini Mexico CDMX office is located on the 9th floor, interior 902, which houses the data center, delivery, administrative, commercial services, call center. The facilities are located at a medium political risk and a medium environmental risk. Economic dynamics change frequently, so this can interfere with Stefanini's operations, and there is also a high risk of protests that can affect access to the facilities, or in the case of Mexico City there are tremors that can affect the building.

The Jaguariuna office has a datacenter located on the first floor, an administrative area and service delivery located on the ground floor of a dedicated building with 2 levels in Jaguariuna, São Paulo, Brazil. This facility is located in a low risk political and low risk environmental location. The government is currently conducting large scale corruption trials and may interfere with economic operations through policies / laws. The facility may be subject to flood threats (roof) and crime, can be a little concern. In addition, movement throughout the city during an emergency situation may have low impact due the low local traffic.

The Santana facility has a datacenter located on the 1st floor and delivery located on the 1st floor of a dedicated, multi-story building in São Paulo, Brazil. This facility is located in a low-medium risk political and low-medium risk environmental location. The government is stable but may interfere with economic operations through policies / laws. The facility may be subject to flood threats and crime, especially robbery, can be a concern. In addition, movement throughout the city during an emergency situation may be difficult.

The Calle 122 office is located between the 5th and 6th floors of a shared building in Bogotá D.C, Colombia. This office has a data center and delivery services on the 6th floor, and the administrative area on the 5th floor. The facilities are located at a medium political risk and a low environmental risk. Economic dynamics

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 225

change frequently, so this can interfere with Stefanini's operations, and there is also a high risk of protests that can affect access to the facilities.

The Montevideo office is located on the eighth floor of a shared multi-story building in Montevideo, Uruguay. This facility is located in a low-risk environmental and political location. The economic dynamics are pretty basic.

As a global provider of services to multiple clients, Stefanini is bound by the contractual requirements of our clients and the legal requirements of the countries our clients operate in. This includes data privacy, including EU Data Protection (GDPR), Brazil Data Protection (LGPD) and Australia Data Privacy laws, HITECH (HIPAA) laws, and additional laws our customers may be bound by (whether noted in contractual language or not).

As a data hosting company, Stefanini has IT equipment that is placed in locations (DMZ) where external attackers could try to cause data leakage or system disruption.

4.2. Understanding the needs and expectations of interested parties

Stefanini determined clients, employees, top management and community obligations (national, international) with legal requirements as interested parties that are relevant to the information security management system. These requirements are determined as described in ISMS-005 Procedure, Identification of Requirements.

4.3. Certification Scope for ISO 27001:2013

Stefanini determined the boundaries and applicability of the information security management system as it relates to certification to the ISO 27001:2013 standard:

Information security system for the protection of external customer proprietary information held within Stefanini's servers and datacenters located in Bucharest (Romania), Sibiu (Romania), Southfield (Michigan/USA), Manila (Philippines), Dalian (China), Chișinău (Moldova), Noida (India), Hyderabad (India), Mexico City (Mexico), Bogotá (Colombia), Montevideo (Uruguay), Santana- São Paulo (Brazil) and Jaguariúna - Sao Paulo (Brazil – Head Office).

4.4. Information security management system

Stefanini established, implemented, maintains and continually improves the information security management system, in accordance with the requirements of ISO 27001.

5. Leadership

5.1. Leadership and commitment

By the authority of the Global Chief Executive Officer, the Security Governance Committee (SGC) is a Stefanini group which recommends solutions related to establishing and monitoring site-wide security policies, regulations, guidelines, standards, and priorities and performing other duties as assigned. This group identifies and assesses local security, privacy and compliance needs and assists with their development and implementation.

The group works with the Information Communication Technology (ICT) organization and other support departments to review progress on security initiatives, to provide feedback, to make recommendations, and to serve as a forum for communication with the organization at-large. At both strategic and tactical levels, the

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 226

group serves as an important touch point to ensure that the actions of one information technology organization do not cause unnecessarily adverse impacts on another.

This group functions at a local level, depending upon the organization responsible for in-scope infrastructure. There are two SGC's defined, the Northern Hemisphere Security Governance Committee and the Southern Hemisphere Governance Committee. They will serve the role as "Top Management" where documented in the ISMS. Please refer to Appendix A for further charter information.

Top management demonstrates leadership and commitment to the information security management system by:

a) ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization;

b) ensuring the integration of the information security management system requirements into the organization's processes;

c) ensuring that the resources needed for the information security management system are available;

d) communicating the importance of effective information security management and of conformity to the information security management system requirements;

e) ensuring that the information security management system achieves its intended outcome(s);

f) directing and supporting people to contribute to the effectiveness of the information security management system;

g) promoting continual improvement;

h) supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

5.2. Policy

Top management established an information security policy according to *ISMS-001 Policy, Information Security.*

This policy is available as documented information, it is communicated within the organization and it is available to interested parties.

5.3. Organizational roles, responsibilities and authorities

Top management ensures that the responsibilities and authorities for roles relevant to information security are assigned and communicated.

Top management assigns the responsibility and authority for ensuring that the information security management system is in conformity with the requirements of the International Standard and for receiving reports on the performance of the information security management system.

6. Planning

6.1. Actions to address risks and opportunities

6.1.1. General

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 227

When planning for the information security management system, the organization considered the issues faced by the organization, the needs and context of the organization, and the expectations and requirements of interested parties. Stefanini determined the risks and opportunities that needed to be addressed to ensure that the information security management system could achieve its intended outcome and prevent, or reduce, undesired effects, in order to achieve continual improvement.

The organization's planned actions include addressing these risks and opportunities, integrating and implementing the actions into its information security management system processes and evaluating the effectiveness of these actions.

This process is performed as described in *ISMS-020 Procedure, Risk Treatment Plan.*

6.1.2. Information security risk assessment

The organization defined and applied an information security risk assessment according to *ISMS-019 Procedure, Risk Analysis.*

6.1.3. Information security risk treatment

The organization defined and applied an information security risk treatment process according to *ISMS-020 Procedure, Risk Treatment Plan.*

In addition to the controls defined on the risk treatment, Stefanini implemented controls as directed in the *ISMS-003 Statement of Applicability*.

The Statement of Applicability contains the necessary controls and justification for inclusions, whether they are implemented or not, and the justification for exclusions of controls.

The organization formulated an information security risk treatment plan according to *ISMS-020 Procedure, Risk Treatment Plan.*

6.2. Information security objectives and plans for their achievement

The organization established information security objectives for relevant functions and levels.

The information security objectives are communicated and updated as appropriate.

When planning on how to achieve its information security objectives, the organization determines corrective or preventive actions according to *ISMS-009 Procedure, Corrective and preventive actions*.

7. Support

7.1. Resources

The organization determines and provides the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system.

7.2. Competence

The organization determines the necessary competence of persons doing work under its control that affects its information security performance and ensures that these persons are competent on the basis of appropriate education, training, or experience;

Where applicable, the organization takes actions to acquire the necessary competence, and evaluates the effectiveness of the actions taken.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 228

The competence is managed as described on *ISMS-015 Procedure, Recruitment* and *ISMS-013 Procedure, Training and awareness.*

7.3. Awareness

Persons doing work under the organization's control are aware of the information security policy, their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance and the implications of not being in conformity with the information security management system requirements.

Awareness and training actions are performed as described on *ISMS-013 Procedure, Training and awareness*.

7.4. Communication

The organization determined the need for internal and external communication relevant to the information security management system.

Internal communication on the ISMS is performed according *to ISMS-013 Procedure, Training and awareness* and *ISMS-003 Statement of Applicability*.

External communication on the ISMS is performed on the web site, Confidentiality agreement with suppliers and Contractual documents.

Stefanini maintain contact with special interest groups by appropriate contacts with specialist forums and professional associations. These contacts are made through Stefanini´s expertise and recorded on meeting minutes or evidences of participation in forums or meetings or workshops. These records are maintained as defined on the *ISMS-013 Procedure, Training and awareness,* and knowledge or by the person in charge, as appropriate. The information to be communicated, as well as the criteria, are indicated in the following table:

Information	When to Communicate	Who to Communicate	How to communicate	How to Register
Information Security Policy	In admission of new personnel	All the staff	Organizational On-boarding	On-boarding registration by RH
Information Security Policy	All the time	Public	Available on intranet / company site	No need registration
Responsibilities and Authorities	In admission of new personnel	All the staff	Through procedures, processes	On-boarding registration by RH
Risks and Opportunities	When a new risk is identified / changed	All personnel involved in the Information Security System	By e-mail / conferences anytime Regular Meetings of the Security Governance Committee. Management Review	Risk matrix
Applicable Legal Requirements	At the time of identification of the requirement and definition of the form of compliance	All personnel involved in complying with the legal requirement	Internal on-boading involved with compliance with legal requirements or in the definition of specific processes and / or procedures	On-boarding registration by RH
ISMS Processes and Procedures	In admission of new personnel. In cases of process and / or procedure changes	All personnel involved with the process and / or procedure	Organizational On-boarding On-boarding Internal Change Disclosures	On-boarding registration by RH Disclosures Records

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 229

ISMS Indicator Results	In Regular meetings of the Security Governance Committee	Security Governance Committee, Top Management	Regular Meetings of the Security Governance Committee. Management Review	ISMS Portal

7.5. Documented information

7.5.1. General

The organization's information security management system includes documented information required by ISO 27001 and documented information determined by the organization as being necessary for the effectiveness of the information security management system.

7.5.2. Creating and updating

When creating and updating documented information the organization ensures appropriate identification and description, in appropriate format and media, and review and approval for suitability and adequacy.

7.5.3. Control of documented information

Documented information required by the information security management system and by ISO 27001 is controlled according to *ISMS-006 Document and Record Control procedure*.

Documented information of external origin, determined by the organization to be necessary for the planning and operation of the information security management system, is identified as appropriate and controlled.

8. Operation

8.1. Operational planning and control

The organization plans, implements and controls the processes needed to meet information security requirements, and implements actions to address risks and opportunities. The organization implements plans to achieve information security objectives.

The organization keeps information documented to the necessary extent to have confidence that the processes have been carried out as planned.

The organization controls planned changes and reviews the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.

The organization ensures that outsourced processes are determined and controlled.

8.2. Information security risk assessment

The organization performs information security risk assessments at planned intervals or when significant changes are proposed or occur, taking into account the criteria established in *ISMS-019 Procedure, Risk Analysis.*

The organization retains documented information of the information security risk assessments results.

8.3. Information security risk treatment

The organization implements the information security risk treatment plan.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 230

The organization retains documented information of the information security risk treatment results.

9. Performance evaluation

9.1. Monitoring, measurement, analysis and evaluation

The organization evaluates the information security performance and the effectiveness of the information security management system.
For the Northern Hemisphere Security Governance Committee, the Quality Manager and ICT Risk Manager will act as the Top Management Representatives. For the Southern Hemisphere Security Governance Committee, The Governance and PMO Executive Manager will act as the Top Management Representative and as the Corporate Top Management Representative, consolidating all the results on ISMS. Colombia, Mexico and Uruguay have local representatives of Senior Management.

This role, independent of other activities, is responsible for implementing and maintaining the Information Security Management System according to ISO 27001 and reporting the ISMS performance to the members of Top Management ensuring awareness of all organizational security topics related to clients' requirements

The organization determines the operational controls and measures the results in order to take actions that correct or improve the performance or effectiveness of the ISMS. In reviewing key metrics, if a metric fails to meet target for two consecutive months, a corrective action should be created. These actions are handled according to *ISMS-009 Procedure, Corrective and preventive actions.*

The organization retains appropriate documented information as evidence of the monitoring and measurement results.

9.2. Internal audit

The organization conducts internal audits according to *ISMS-008 Procedure, Internal audit.*

The organization retains documented information as evidence of the results of internal audits.

9.3. Management review

Top management reviews the organization's information security management system according to *ISMS-007 Procedure, Management review.*

The organization retains documented information as evidence of the results of management reviews.

10. Performance evaluation

10.1. Nonconformity and corrective action

When a non-conformity occurs, the organization acts according to the Non-conformity process.

Corrective actions are appropriate to the effects of the nonconformities encountered.

The organization retains documented information as evidence of the nature of the nonconformities, of any subsequent actions taken and the results of any corrective action.

10.2. Continual improvement

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 231

The organization continually improves the suitability, adequacy and effectiveness of the information security management system.

11. Managing records kept on the basis of this document

- Not applicable

12. Document management

The owner of this document is the Top Management Representative, who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria must be considered:

- Standard review
- Results of internal audit

A current version of this document is available to all staff and under version control on the corporate document control system.

13. Appendices

- Appendix A: Security Governance Committee Charter

14. Change history

Date	Version	Created by	Description of change
22-JAN-2014	1.0	Larissa Longo	Document creation
28-AUG-2014	2.0	Matthew Engler	Updated Context and Scope
08-SEP-2015	3.0	Matthew Engler	Clarified ISMS Certification Scope versus general applicability
23-AGO-2016	4.0	Matthew Engler	Updated Context and Scope
10-JUL-2017	5.0	Matthew Engler	Updated Context and Scope
5-SEP-2019	6.0	Matthew Engler	Updated External Context
21-DEC-2019	7.0	Licsileth Palma	Updated context and scope. Communication criteria table is included
01-JUL-2020	8.0	Elaine Pinheiro	Updated Context and Scope

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 232

Appendix A: Security Governance Committee Charter

Committee

By the authority of the Global Chief Executive Officer, the Security Governance Committee (SGC) is a Stefanini group which recommends solutions related to establishing and monitoring site-wide security policies, regulations, guidelines, standards, and priorities and performing other duties as assigned. This group identifies and assesses local security, privacy and compliance needs and assists with their development and implementation.

The group works with the Information Communication Technology (ICT) organization and other support departments to review progress on security initiatives, to provide feedback, to make recommendations, and to serve as a forum for communication with the organization at-large. At both strategic and tactical levels, the group serves as an important touch point to ensure that the actions of one information technology organization do not cause unnecessarily adverse impacts on another.

Scope of Topics Considered

The scope of this committee is security and compliance issues as related to ICT governance. These issues may include but are not limited to:

- Business continuity
- Management of risks, assets and data
- Security policy
- Compliance with security provisions in acts, regulations and agreements
- Identity and access management (IAM)
- Security technology
- Incident management and response
- Training, awareness, and documentation

Charge

Committee members will raise security-related issues and participate in discussions to formulate recommendations with a holistic perspective on the organization's needs. The SGC is charged with:

- Sponsoring and/or approving security-related policies, standards or procedures at Stefanini.
- Reviewing, assessing, and prioritizing proposals for new security initiatives.
- Formulating security strategies and/or processes, as well as ad hoc task forces or working groups, as necessary, for the review and adoption of appropriate policies, standards or procedures.
- Ensuring security strategies align with Stefanini's mission and objectives as well as comply with applicable laws, regulations, and requirements.
- Recommending procedures that enhance Stefanini's business continuity and resiliency.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 233

Membership

The governance committee represents the business and technology management personnel aligning the goals of the Risk and Information Security organization with those of the business. It is made up of stakeholders within the organization and should include membership from the following areas:

- ICT
- Service Delivery
- Human Resources
- Finance and Business
- Office of General Counsel

All members will serve on a permanent basis. The committee may appoint additional members as needed with appropriate approval.

Meetings

Meetings will follow the requirements documented in ISMS-007, Management Review Procedure. The SGC must meet at least twice per year.

Items Requiring Rapid Response

Although operational staff handles true emergency incident response, there are cases in which the SGC may need to respond to security and privacy issues in short periods of time. If the SGC needs to respond to or to vote on an issue quickly, it can both convene and vote electronically.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 234

BACKUP SYSTEM POLICY

Information Security Management System



Code:	ISMS-004
Version:	8.0
Date of version:	26-AGO-2020
Created by:	Licsileth Palma
Approved by:	Washington Souza
Confidentiality level:	Internal Use

Table of contents

1. PURPOSE, SCOPE AND USERS 4
1.1. Definitions and Abbreviations 4
2. REFERENCE DOCUMENTS 4
3. DESCRIPTION 5
3.1. Scope of Backup 5
3.2. Timing of Backup 5
3.3. Storage of Backups 5
3.4. Restore Testing 5
4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 5
5. DOCUMENT MANAGEMENT 5
6. APPENDIX 1 – NORTHERN HEMISPHERE BACKUP PROCEDURES 7
6.1. Timing of Backup 7
6.2. Scope of Backup 7
6.2.1. Physical Windows Server 7
6.2.2. Physical Linux Server 7
6.2.3. Virtual Windows Server 7
6.2.4. Linux Servers 7
6.2.5. Databases 7
6.3. Supporting Processes 8
6.3.1. Logs 8
6.3.2. Failures 8
6.3.3. Electronic Media Storage 8
6.3.4. Retention 8
6.4. Restore Process 8
6.4.1. Restore Scheduling 8
6.4.2. Restore Testing 8
6.4.3. Requested Restore 8
6.5. Tapes identification 8
7. APPENDIX 2 – SOUTHERN HEMISPHERE BACKUP PROCEDURES 9
7.1. Backup 9
7.2. Data restoration 9
7.3. Tapes identification 9
7.4. Backup Restoration Test 9
8. CHANGE HISTORY 21

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 236

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 237

1. Purpose, scope and users

The purpose of this document is to describe Stefanini´s operations to perform the information backup and recovery. The backups are performed for the company´s vital assets and for information requested by Stefanini´s employees.

This policy applies to Stefanini Employees, sub-contractors, consultants, business associates, and other workers at Stefanini, including all personnel affiliated with third parties and subsidiaries on the Stefanini infrastructure (collectively “User(s)”) working within Northern Hemisphere infrastructure.

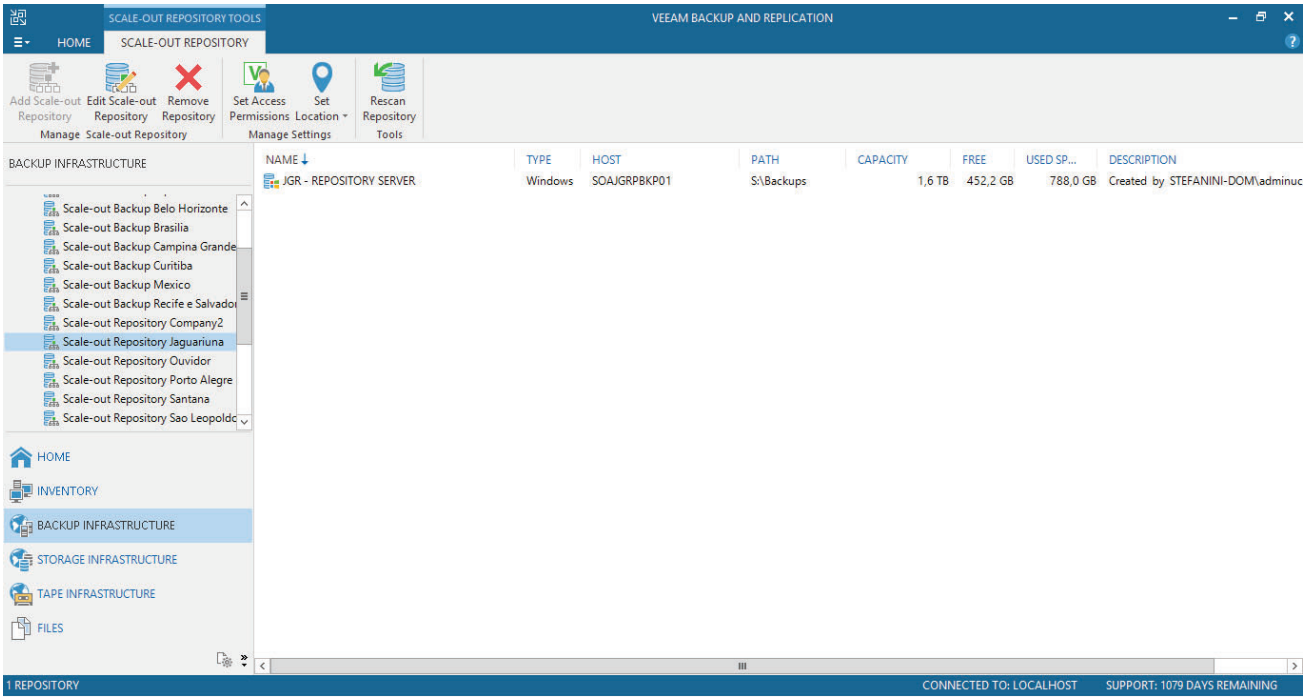
1.1. Definitions and Abbreviations

Incremental Deduplication: Backup of new and modified data, through the agent installed on the servers by Veeam Backup's “Protection Group”

Full: Backup of the server completely virtualized and backed up by Veeam Proxy.

Veeam Backup & Replication: Backup solution used in Stefanini's environment, responsible to comply with the developed policy

Storage Pool (Primary): Physical area on disk where the operations of saving data are made.



Physical & Cloud Infrastructure ((nventory): It is each server involved in the solution to repository creation.

Veeam Software Group GmbH: Veeam Backup & Replication

2. Reference documents

- ISO/IEC 27001 standard, 7.5.3, A. 12.3.1

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 238

- ISMS-001 Policy, Information Security
- ISMS-044 Policy, Use of Cryptographic Controls
- ISMS-045 Policy, Physical and environmental security

3. Description

3.1. Scope of Backup

The Infrastructure Support teams, with input from the Information Security Manager and Asset Owners, are responsible for defining the systems required to be backed up. This will include, by default, all critical information systems and any system containing personally identifiable information.

Where a system contains Restricted information, e.g. Personally Identifiable Information, the backup will be encrypted per *ISMS-044 Policy, Use of Cryptographic Controls*.

3.2. Timing of Backup

All servers to be backed up will receive a full initial backup, at least once a month. All servers will receive a Incremental Deduplication during the executions defined in the schedule, whenever changes in the data saved in the previous executions occur.

A set of Full Backups each month will be keep for one year, unless legal obligations require that this set be maintained longer.

All other “Incremental Deduplication” backup sets will be maintained for one month.

3.3. Storage of Backups

Current backup set will be kept on-site within a secured area as defined in *ISMS-045 Policy, Physical and environmental security*. Backup storage media will be sent off-site at a minimum, weekly.

3.4. Restore Testing

Minimum restoration test is completed on selected systems four times a year, remembering that these requests can occur through the ticket tool requesting data restoration and thus ensure the integrity of data saved.

This includes that files are restored and the system owners validate the results.

4. Managing records kept on the basis of this document

- Not applicable

5. Document management

The owner of this document is the Infrastructure and Support Analyst who must check and, if necessary, update the document at least once a year.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 239

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

- number of incidents related to backup
- number of restore request
- change of technology

A current version of this document is available to all staff and under version control on the corporate document control system.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 240

6. Appendix 1 – Northern Hemisphere Backup Procedures

6.1. Timing of Backup

- All servers will receive an automated incremental backup four nights of the week followed by one full backup.
- All Servers will receive a full backup, at least weekly.

6.2. Scope of Backup

The backup is executed through market standard backup utility. The backup is performed by ICT Management professional. The backup routines may be different due to the server's content.

6.2.1. Physical Windows Server

- System State and All Local Drives

6.2.2. Physical Linux Server

- All Local Drives
- Standard Exceptions:
  - /proc
  - /sys
  - /dev/
  - /lost+found
  - /media
  - /mnt (selectively, to exclude potential network mounts)
  - Custom exclusions based on vendor recommendations

6.2.3. Virtual Windows Server

- Server image + File restore

6.2.4. Linux Servers

- Server image + File restore

6.2.5. Databases

- Option A - DBA will dump the database to a flat file which will then be backed up during the All Local Drives Backup.
- Option B - DB backup agent will be utilized to backup databases.
- If option A is used, the All Local Drives Backup is not to occur until after the Database dump has concluded. Timings will be arranged with the Database Administrator (DBA).
- Standard database exception list will include all *.mdb and *.ldf files.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 241

6.3. Supporting Processes

6.3.1. Logs

An automatic electronic log is kept showing the success or failure of backups. Reports against this log are run from the Backup Administration Console. Backup logs are maintained for a minimum of 30 days. See work instructions for more details on backup logs.

6.3.2. Failures

In the event of a failure, the backup job is rescheduled and if successful then no further steps will be required. In the event of multiple failures of a single server it is expected that further steps will be taken to determine the cause of the failures. An Incident will be opened in the Stefanini Service Desk (eSSD).

6.3.3. Electronic Media Storage

- Local Storage: Current backup set will be kept onsite.
- Off-site storage: Stored in off-site facility in cases.
- Tapes will be picked up and dropped off once a week.
- A log of what cases belong to the correct week's backup is kept.

6.3.4. Retention

- Monthly backup sets, covering the first calendar week starting Wednesday (Week 1), are retained for a period of one year. These backup sets will be over written every 12 months.
- Weekly backup sets, which occur every week with the exception of the first calendar week of the month (Week 2 – 5), are over written every month.

6.4. Restore Process

6.4.1. Restore Scheduling

The Risk Management group, along with the Infrastructure team, will create a schedule for restore testing. This will be monitored by the Business Continuity resource.

6.4.2. Restore Testing

Quarterly restore testing is done for client systems. A Request is submitted along with a document of the systems/ files to be restored. Once the files are restored the system owners validate the results.

Restore testing shall include, at least annually, one database restore and file level restore.

6.4.3. Requested Restore

If a Request / Incident is received during a given month, that restore will be tracked in the restore log and it will be counted as a test of restore on that server for a given period. A record of requested data restores will be logged

6.5. Tapes identification

Tapes will be marked with a unique identifier maintained by ICT Personnel.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 242

7. Appendix 2 – Southern Hemisphere Backup Procedures

7.1. Backup

The backup is performed through Veeam Backup & Replicationmarket solution. The data is executed and stored in Backup Repositories (Primary): Physical area on disk where data save operations are performed. Periodically, by schedule job, the backups are sent to the LTO model tapes. This systematic is performed for files, projects and Database maintained on the network, except for Operating Systems and Programs installed on the servers. The backup system is performed by a professional in the server management area. Backup routines are created respecting the content of each server.

When the person responsible for the application identifies the need for a database backup, it must request a call to the area responsible for the database to perform a "dump" in a dedicated area on the network server.

Servers with user files, systems development, database and e-mail have:

- Daily backup with 30 days restores points (Daily):: Incremental method deduplicated - run from Monday to Friday;
- Monthly backup with 365 days retention (Monthly): Full tape backup method - executed in the first week of each month.

7.2. Data restoration

When a Stefanini employee finds the necessity of restoring a file, such employee opens a ticket in the service desk, who sends it to the servers management area, describing the date and/or file to be restored, its path, the period and the necessity.

The analyst who answers the ticket will analyze the conditions for the data return activity and perform the restoration as requested. If the file is not found or there is no possibility of restoring it, the responsible area will inform the requester and close the ticket.

7.3. Tapes identification

The tapes were identified by adopting the following criteria:

- Full nomenclature of 8 alphanumeric characters;
- The first three digits are characters and identify the company´s office. Ex. JGR (Jaguariuna), SAN (Santana) and EUS (EUSEBIO);
- The 3 digits in the middle are numeric and identify the numerical order of the tapes. Ex.001, 010, 014;
- The last 2 digits are alphanumeric and identify the model of the tape unit. Ex. L3 = LTO3 and L5 = LTO5;

Examples of complete nomenclature:

- Tape 02 from Santana, using a LTO3 model, its name would be: JGR002L3

7.4. Backup Restoration Test

In specific periods, restoration tests of files or servers are performed for the verification of data integrity.

For the understanding of our procedures, some important points are specified:

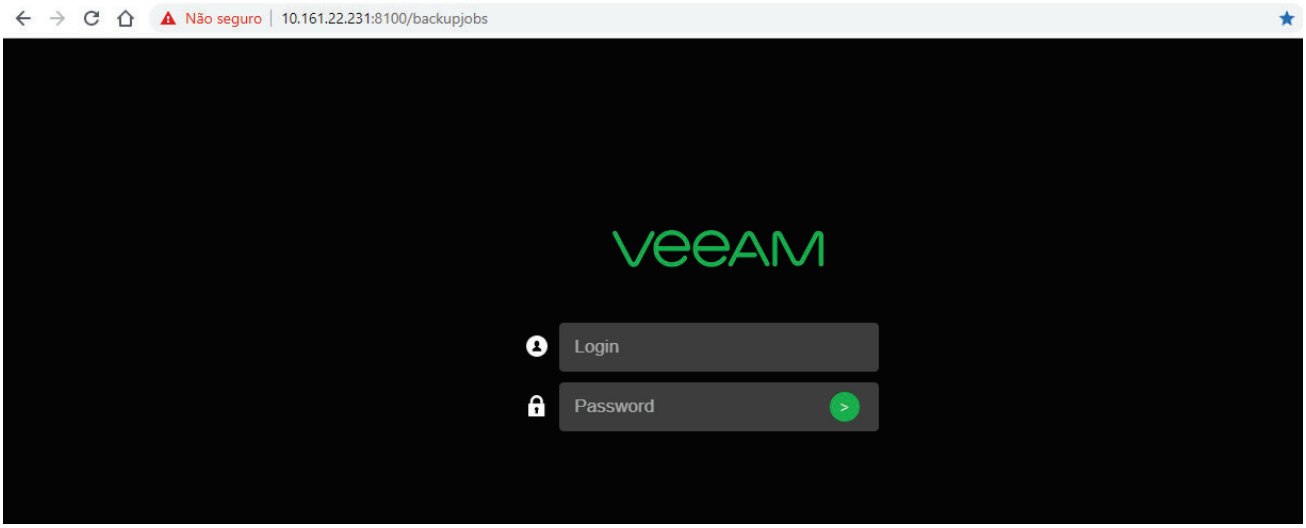
- The test is performed once a month;
- All servers are checked and participate in the restoration test;
- Tests are conducted with a sample of data from each server.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 243

For the performing of the restoration test, the following steps must be performed:

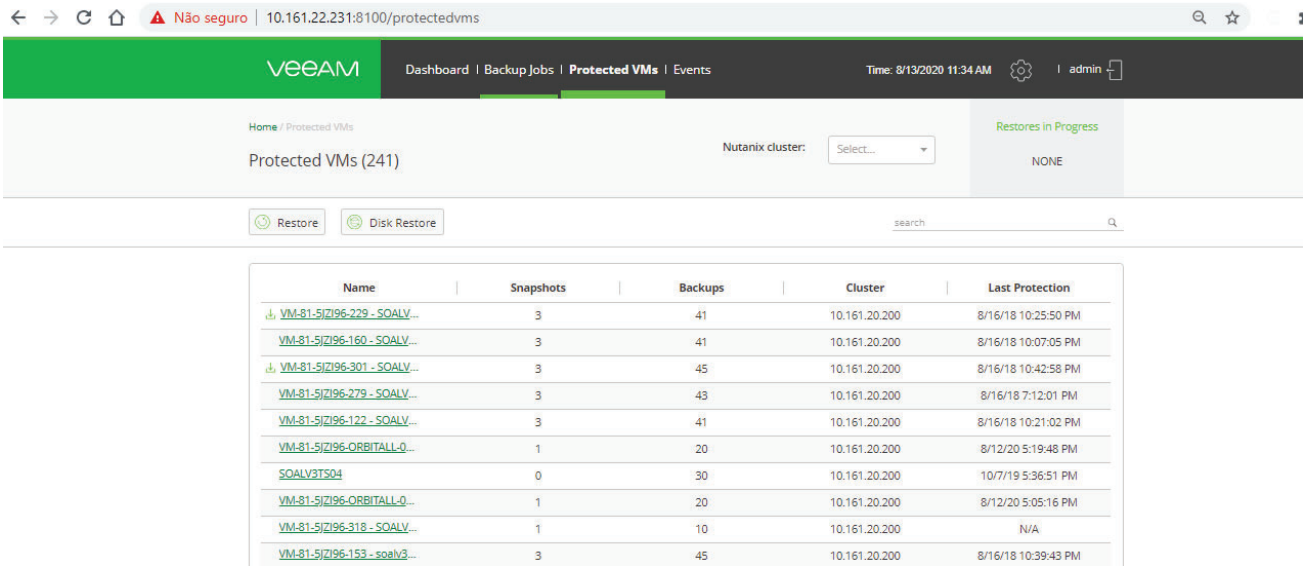
1 - Log into the URI configured to the Veeam Proxy for the performing of backup:

https://10.161.22.231:8100/backupjobs



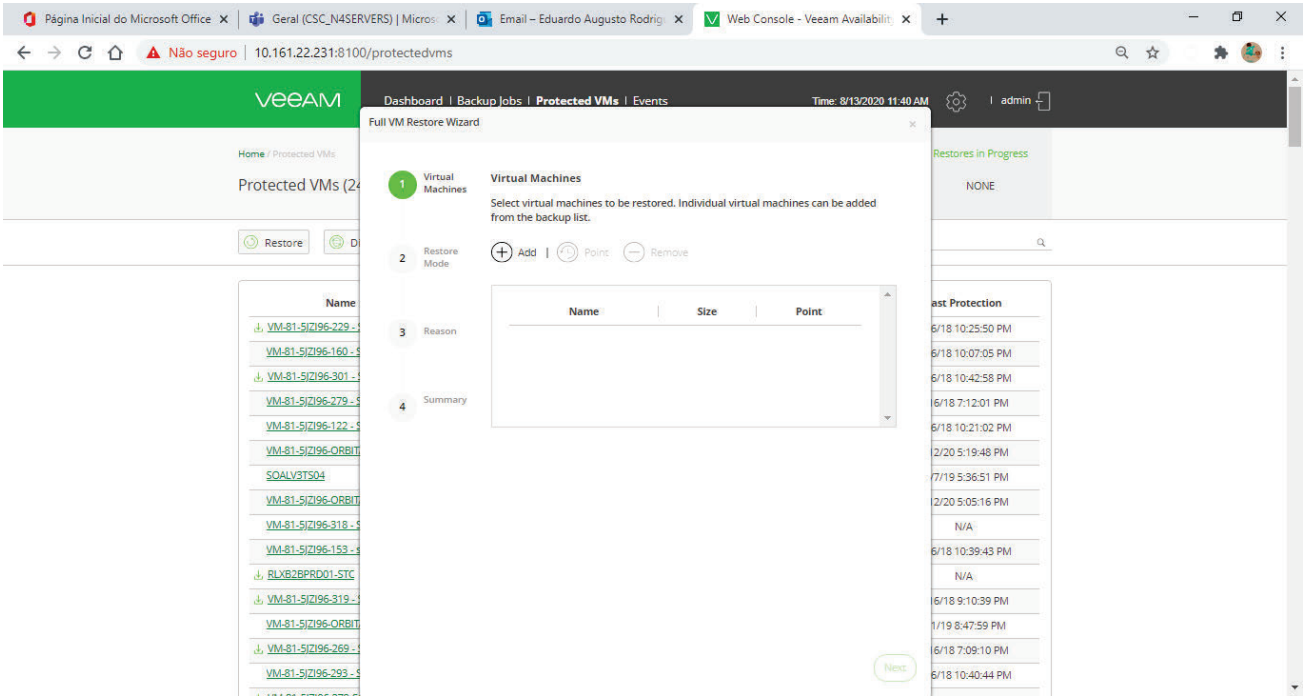
Use Login and Password determined by the backup system administrator.

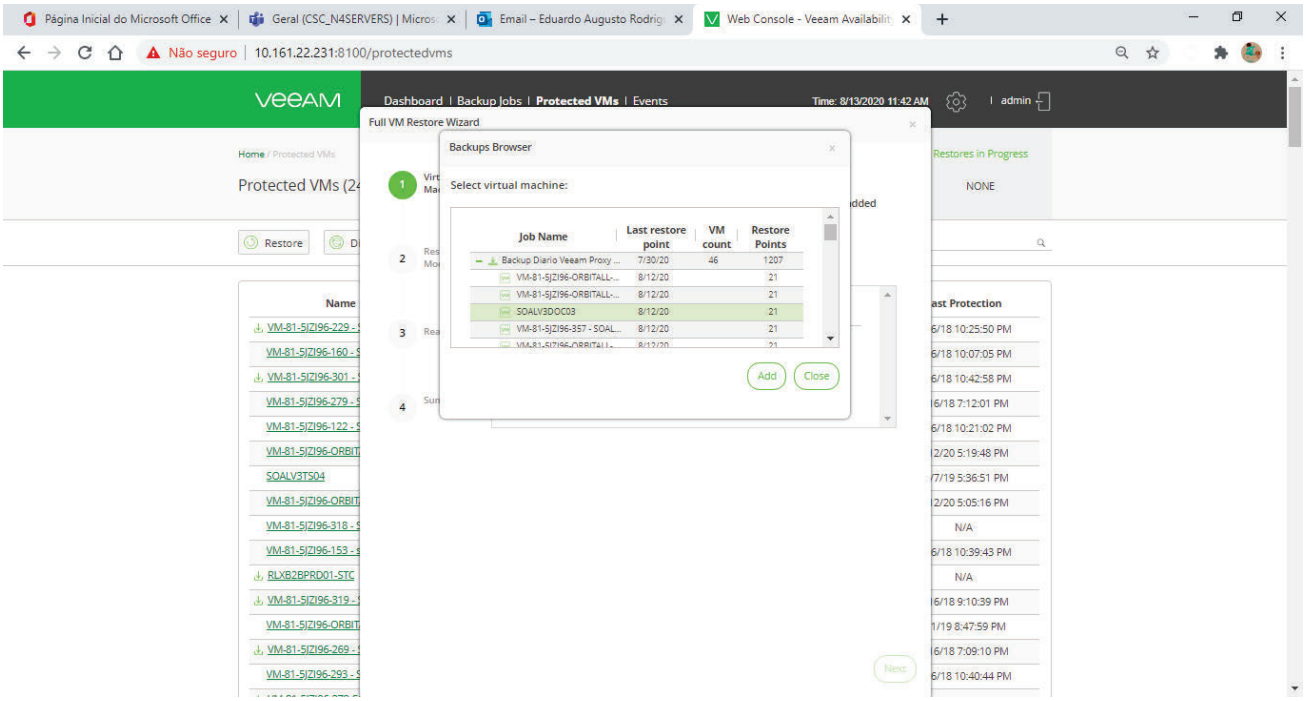
2 - Click on the option Protected VMs then on the button Restore



Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 244

3 – Select the server to restore by clicking the button “Add”

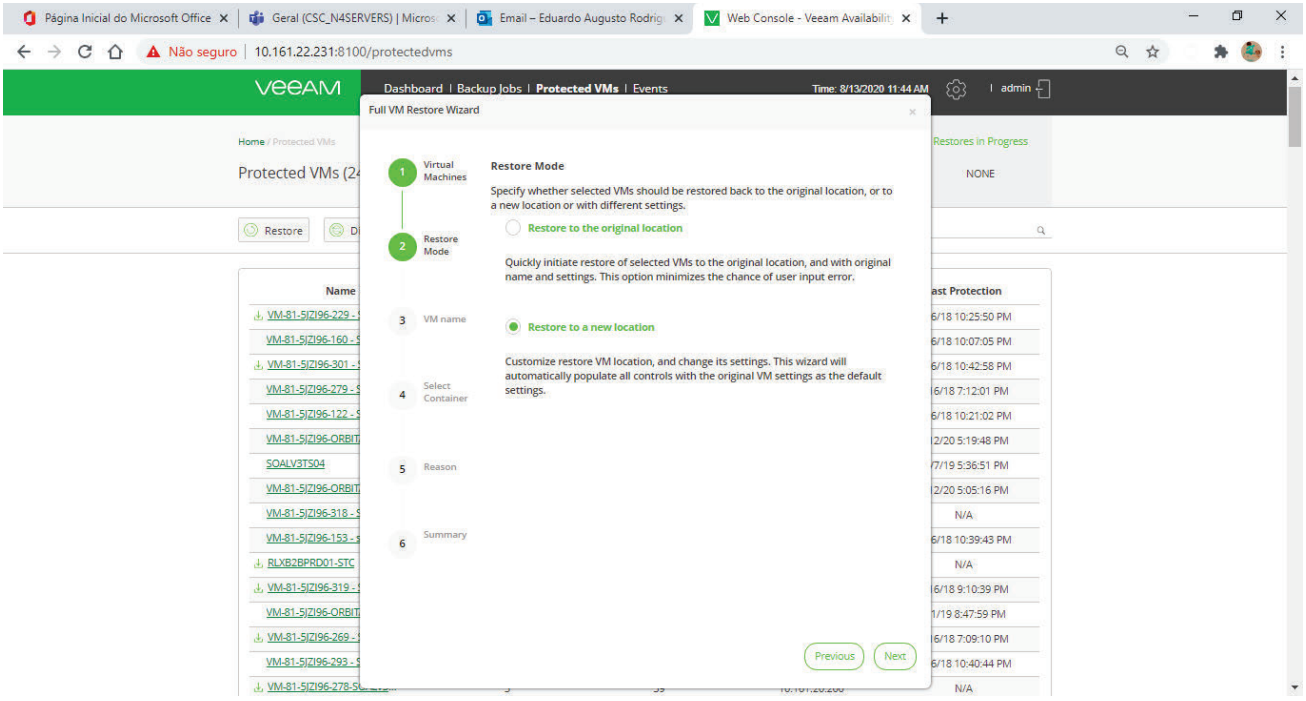




Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 245

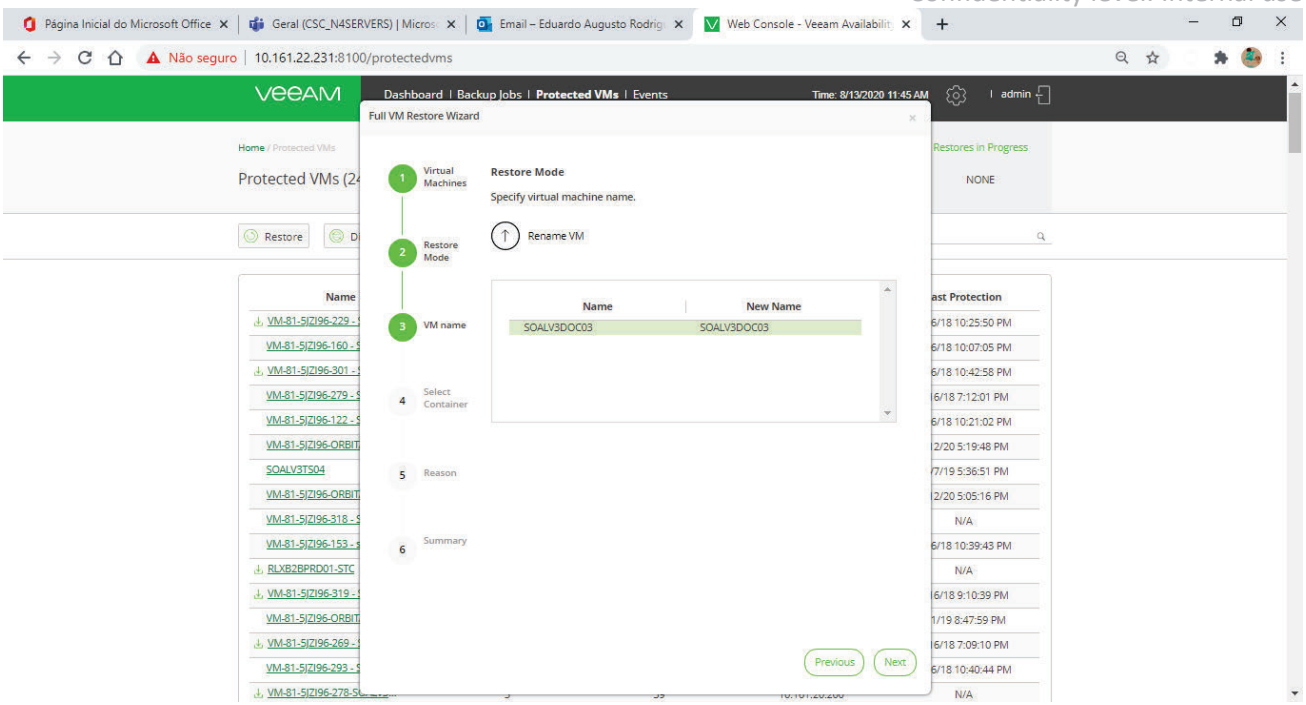
4 – After the desired selection, we can choose the destination of the restoration

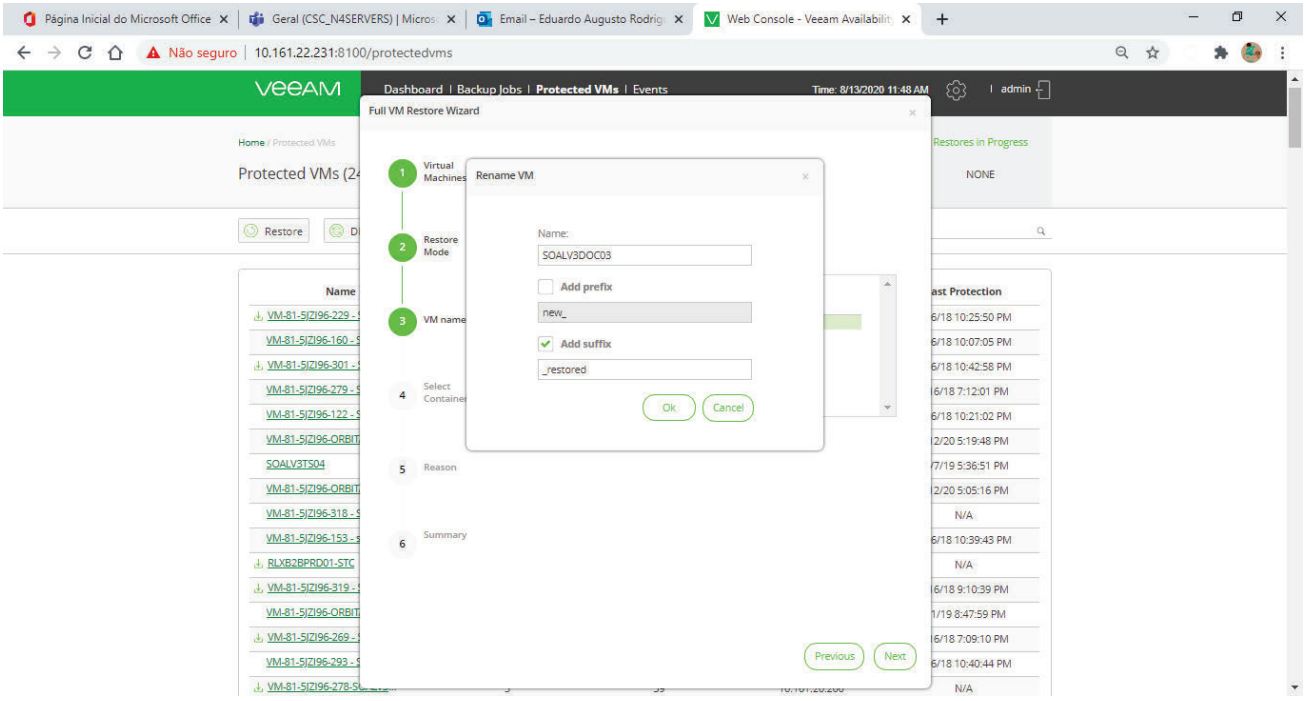
We usually use the option “Restore to a new location”.



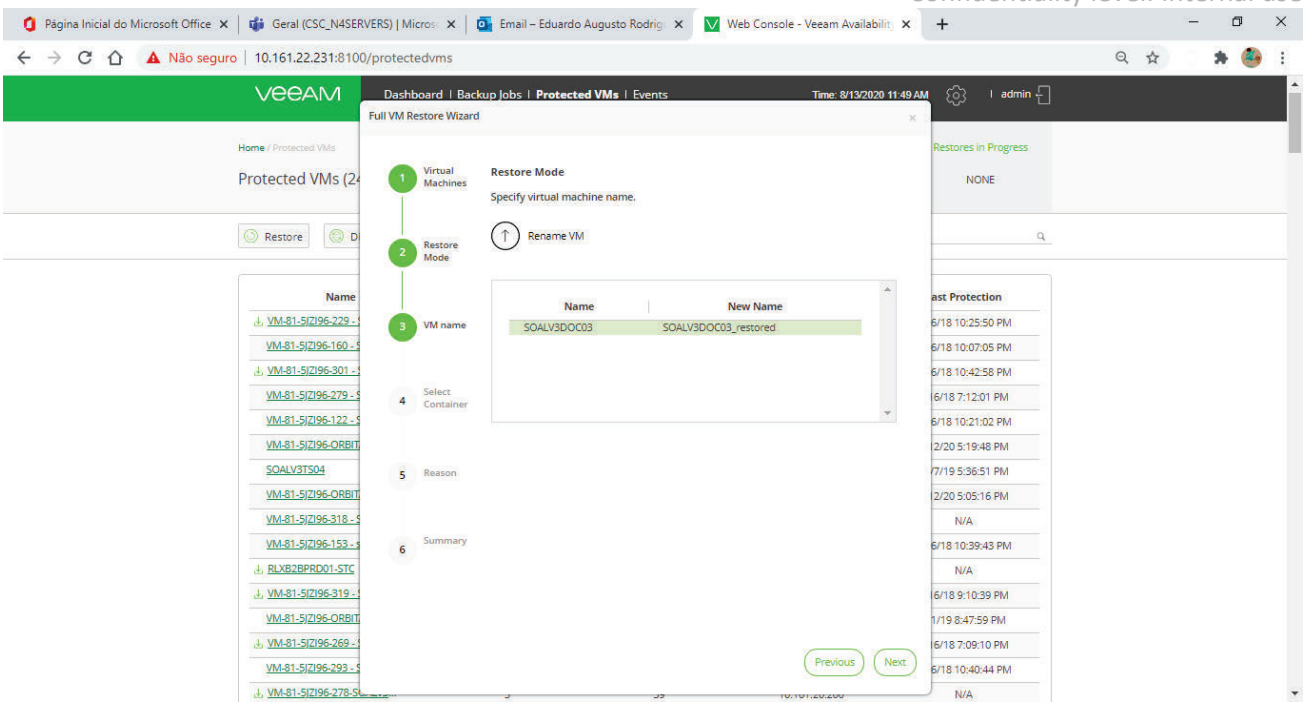
5 – Then we must rename the server to be restored.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 246

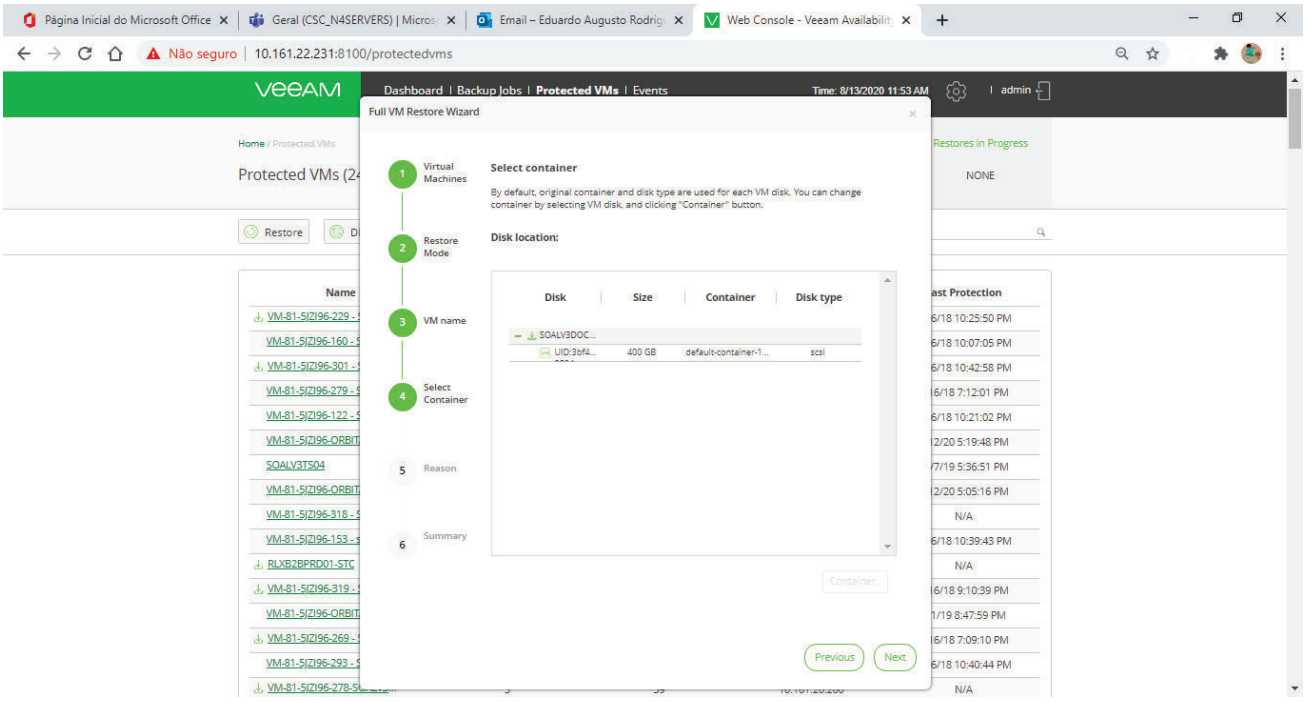




Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 247

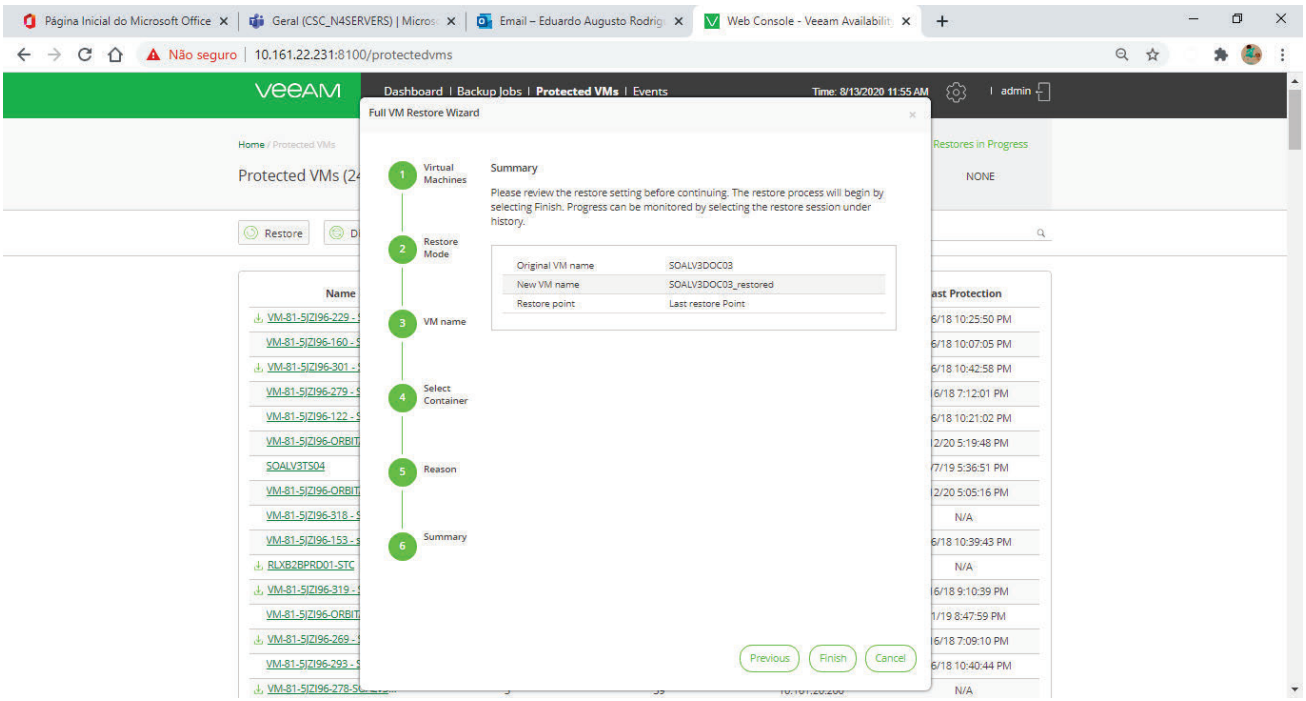


6 – Select the Nutanix Container where the restored VM will be available.



Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 248

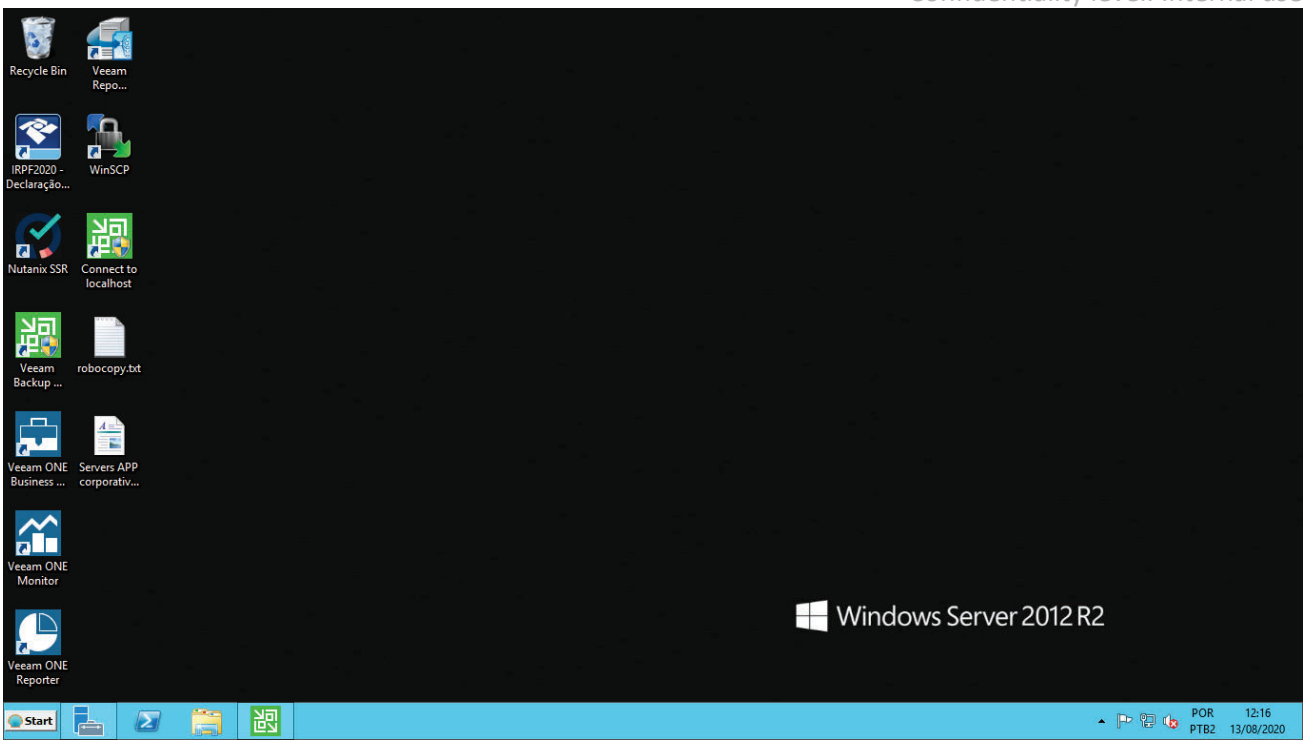
7 - At the end of the configuration of the selected restore, we will click Finish and follow the evolution and implementation of the Restore.



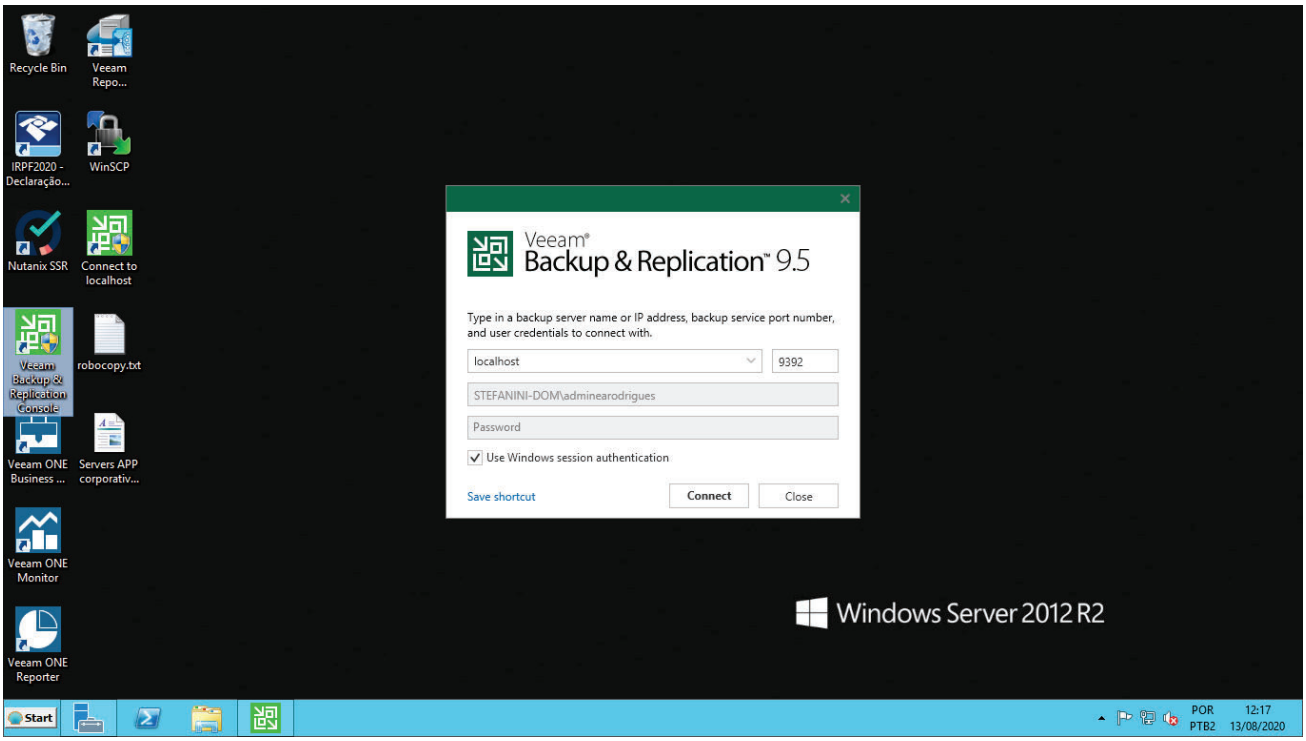
8 – If the restore is requested only for files or folders, the procedure will be through the Protection Group via an agent.

Log on to the Veeam Server with network and domain credentials.

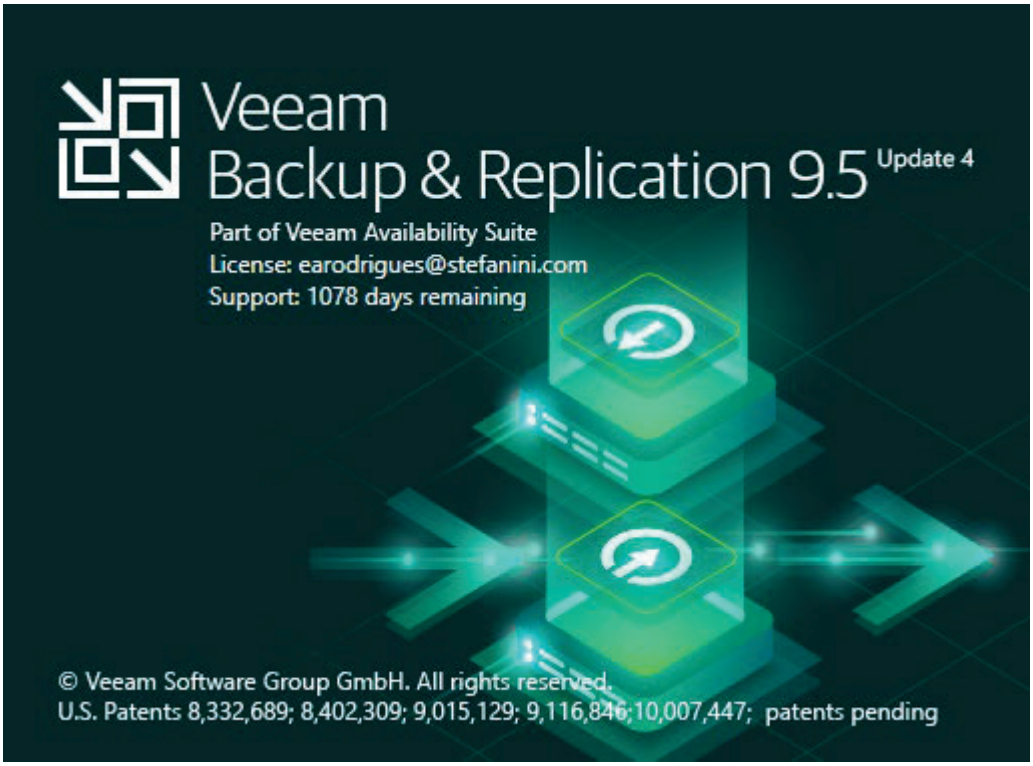
Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 249



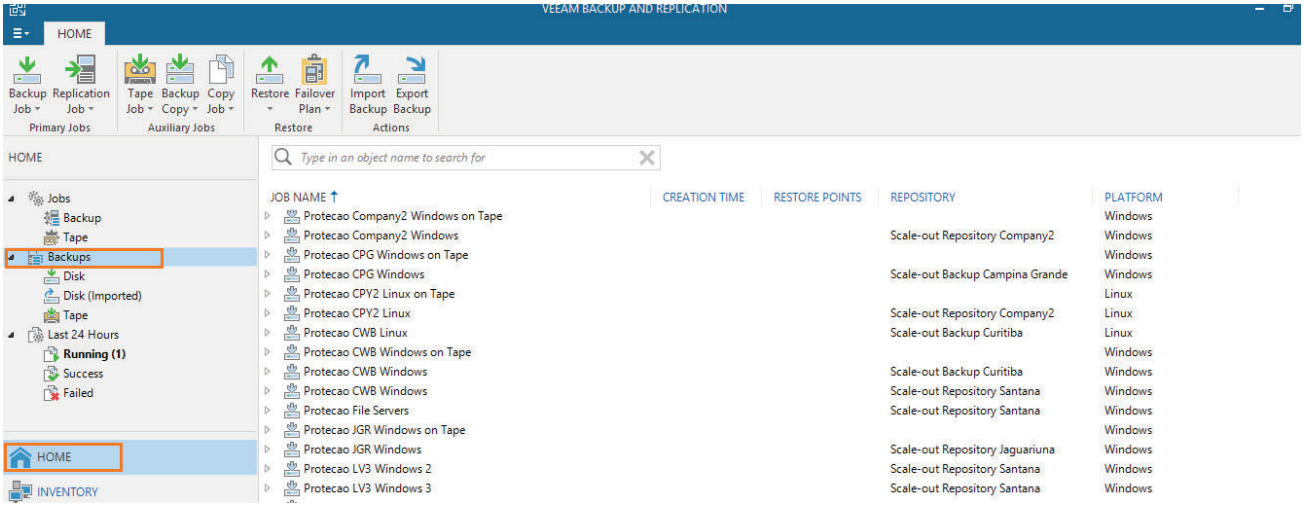
Use the installed application “Veeam Backup & Replication Console” and click Connect



Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 250



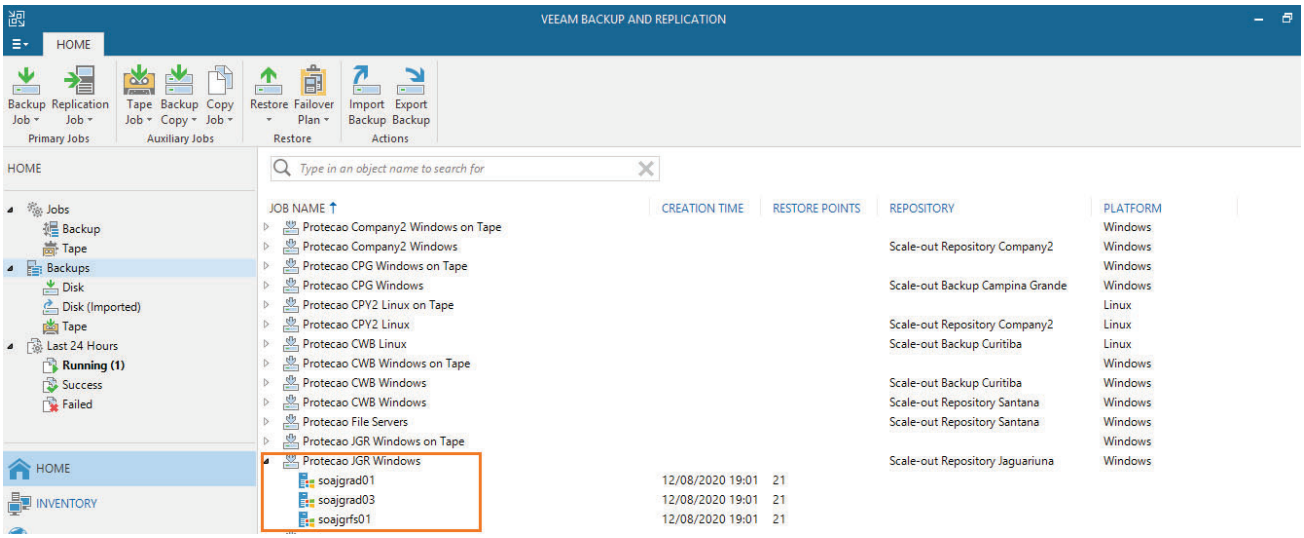
In HOME use the Backups option, according to the print below.



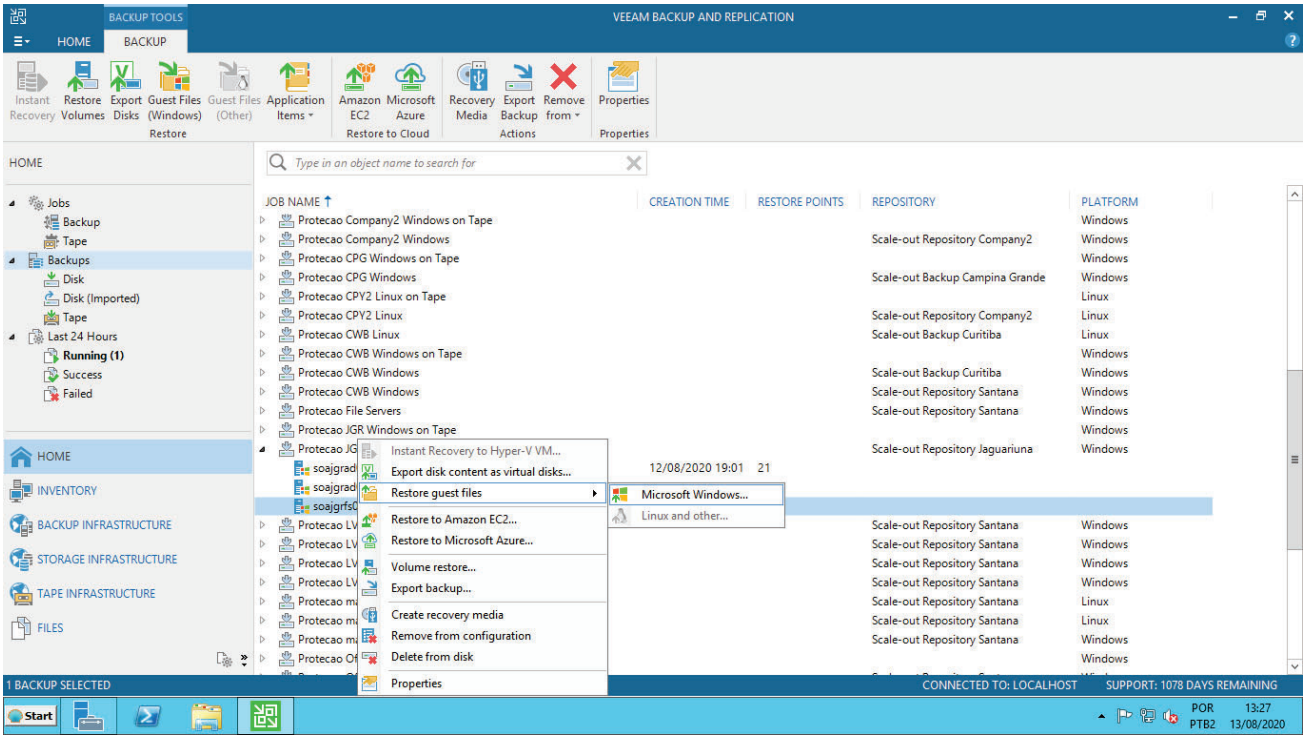
Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 251

Then expand the Jobs that contain the name “Protection”.

These Jobs are the “Protection Group”, intended for backups for granular restoration.

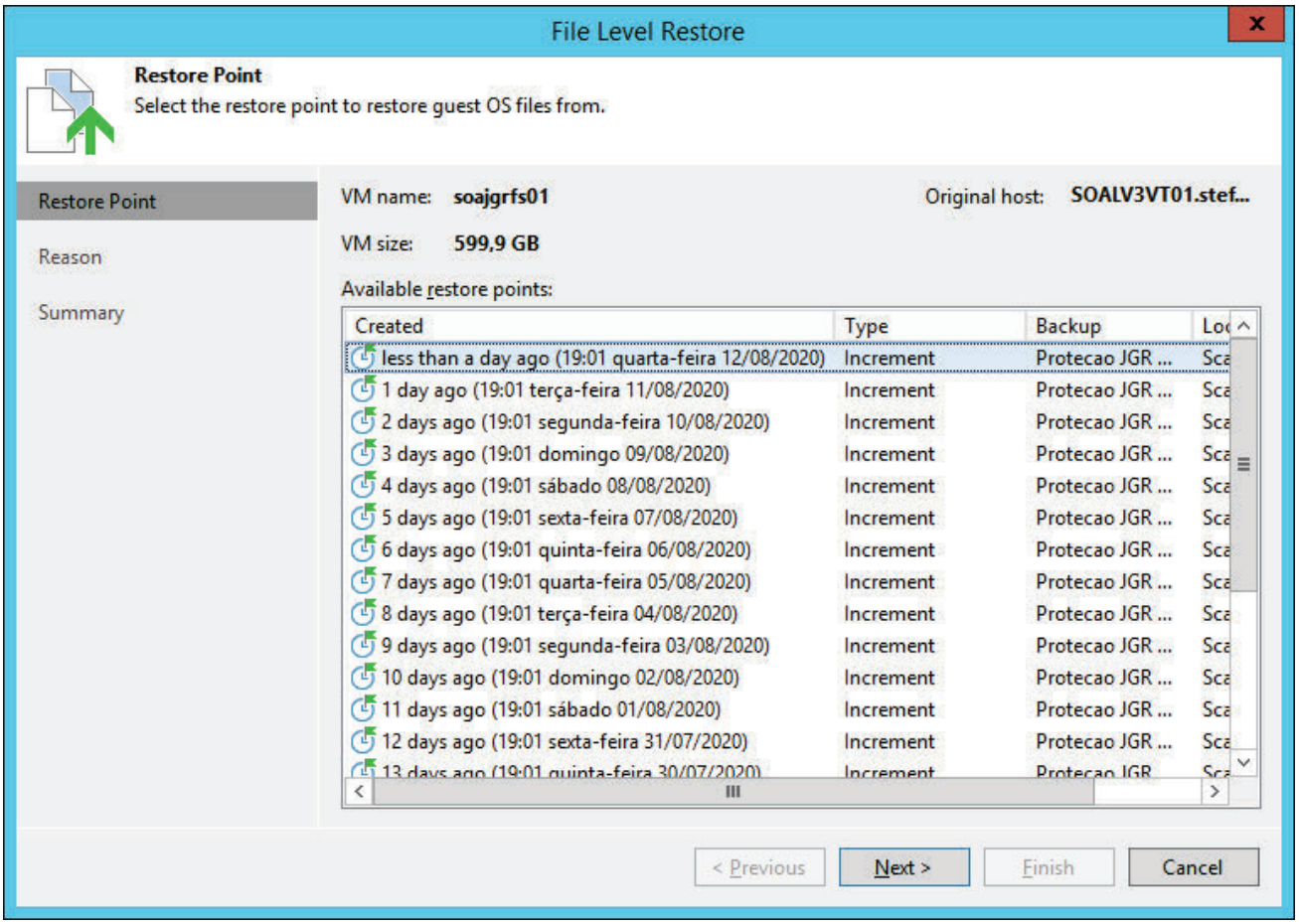


Right-click and select “Restore Guest files” and which operating system the server is running on, in the case below it will be “Miocrosoft Windows”.



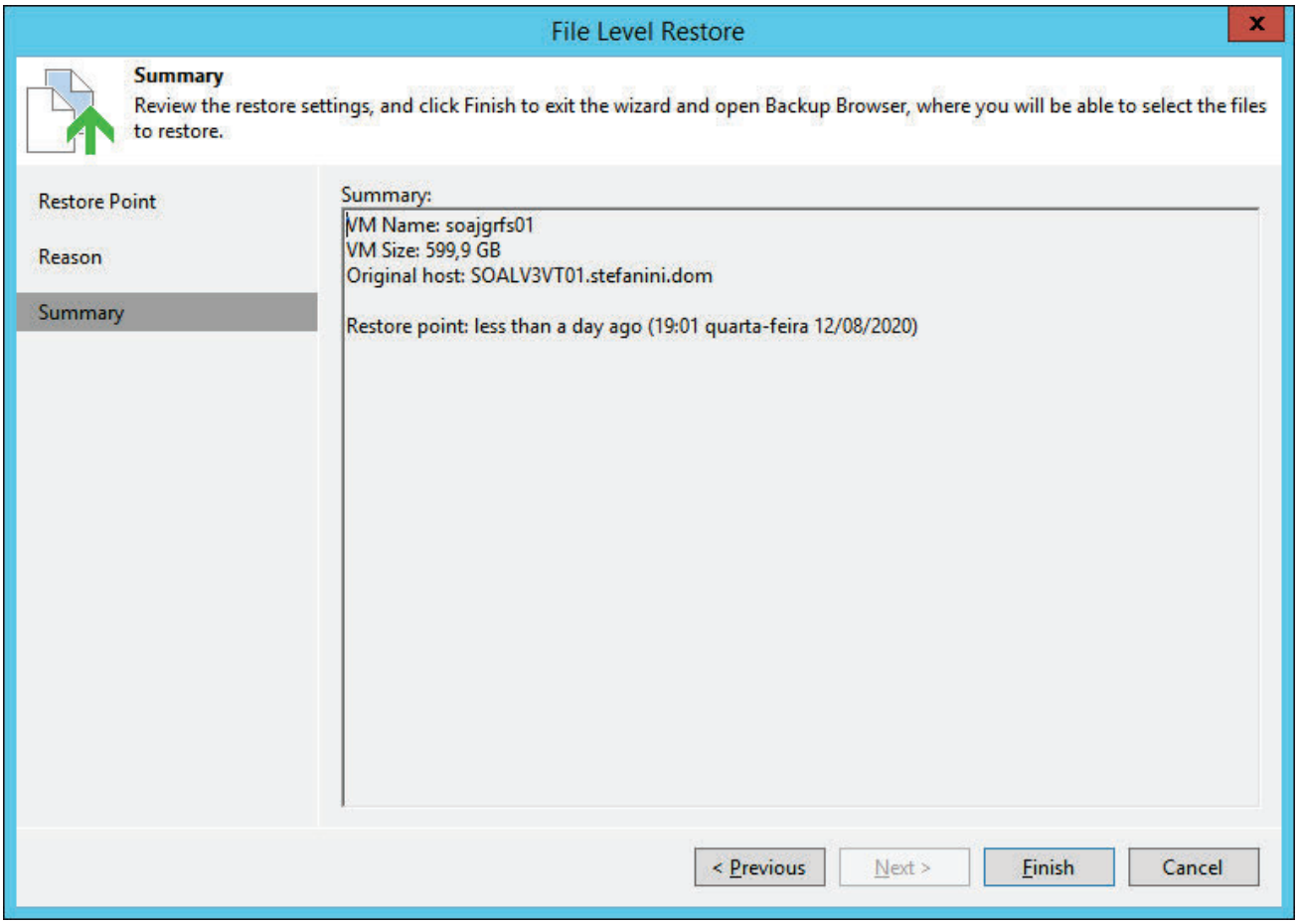
Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 252

Then select what period we should restore from the performed backup.



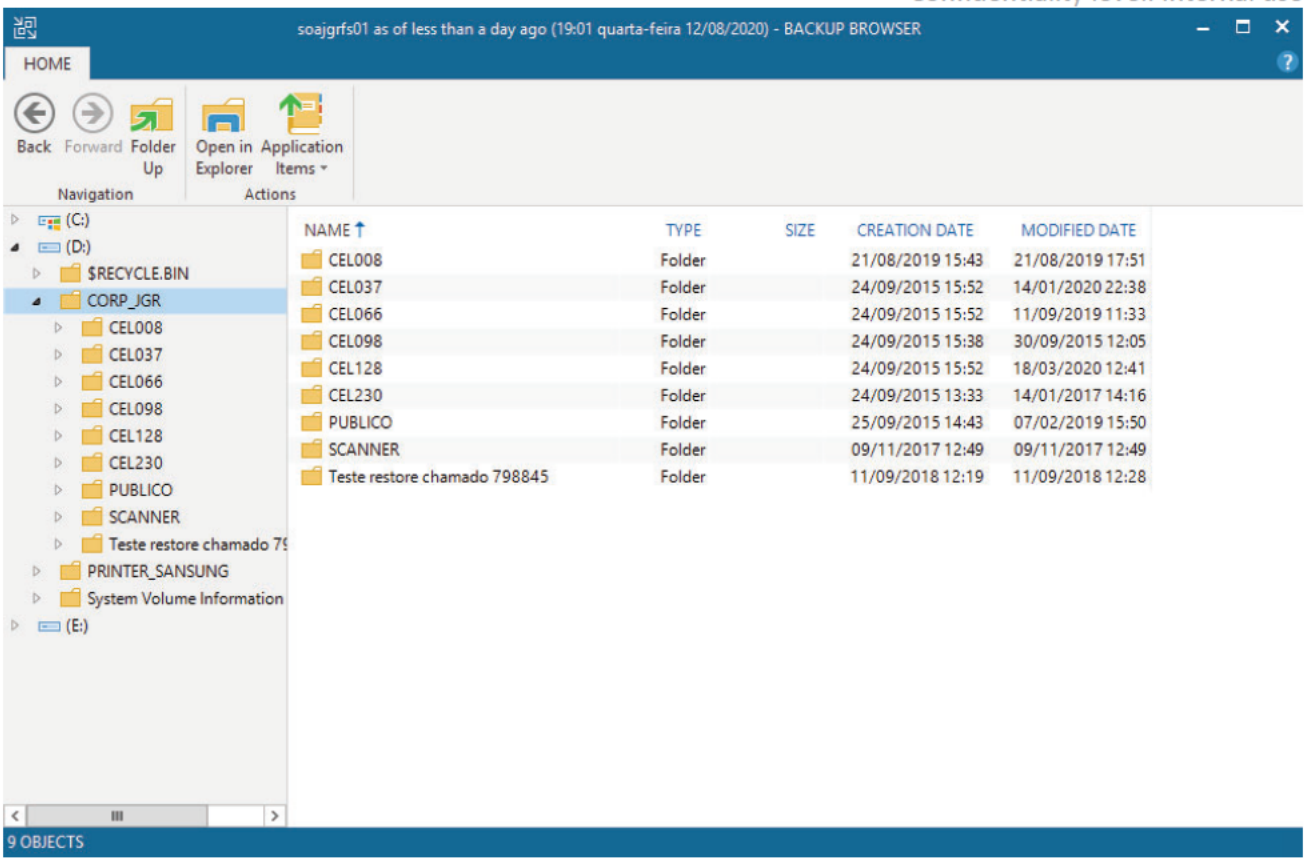
Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 253

Click on Finish to proceed with the customization of the Restore.



Expand the drive where the data is saved and search for the file or folder to be restored.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 254



Note: In Stefanini Colombia there are backup exceptions that are carried out according to the Backup Instructions IN-MA-05.

8. Change history

Date	Version	Created by	Description of change
23/01/2012	1.0 (NH)	Matthew Engler	Document creation
31/01/2014	1.0 (SH)	Luiz Robson	Document creation
01/05/2014	2.0 (NH)	Matthew Engler	Updated to standard formatting
29/08/2014	2.0 (SH)	Sergio Leandro do Nascimento Garcia	Inclusion of the test procedure for backup restoration
11/08/2015	3.0 (Global)	Matthew Engler	Documented global policy; Combined NH and SH procedures as appendices.
21/09/2016	4.0 (Global)	Matthew Engler	Added responsibilities for restore testing and explicit restore tests (NH).
14/07/2017	5.0	Elaine Vanessa	Update procedure.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 255

27/07/2018	6.0 (SH)	Luiz Robson	Added the description of the monthly and annual retention process.
03/08/2020	7.0	Eduardo Augusto Rodrigues	Changes in backup tools and procedures.
26-AUG-2020	8.0	Licsileth Palma	Included for Colombia The instructions to use for the exceptions Backups Instructions IN-MA-05.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 256

IDENTIFICATION OF REQUIREMENTS PROCEDURE

Information Security Management System



Code:	ISMS-05
Version:	2.0
Date of version:	16-SEP-2016
Created by:	Elaine Pinheiro
Approved by:	Washington Souza
Confidentiality level:	Internal Use

Table of contents

1. PURPOSE, SCOPE AND USERS 3

2. REFERENCE DOCUMENTS 3

3. DESCRIPTION 3

3.1. IDENTIFICATION OF REQUIREMENTS AND INTERESTED PARTIES 3

3.2. REVIEWING AND EVALUATION 3

4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 4

5. DOCUMENT MANAGEMENT 4

6. APPENDICES 4

7. CHANGE HISTORY 4

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 258

1. Purpose, scope and users

The purpose of this document is to define the process of identification of interested parties, as well as legal, regulatory, contractual and other requirements related to information security and business continuity, and responsibilities for their fulfillment.

Users of this document are all Stefanini Employees, sub-contractors, consultants, business associates, and other workers at Stefanini, including all personnel affiliated with third parties and subsidiaries on the Stefanini infrastructure (collectively "User(s)") who work on development and maintenance for Stefanini.

2. Reference documents

Documents associated or linked tare listed below:

- ISO/IEC 27001 standard, 4.2, A.18.1.1
- ISMS-001 Policy, Information Security
- ISMS-031 Policy, Business Continuity Management

3. Description

3.1. Identification of requirements and interested parties

Top Management Representative is responsible for identifying (1) all persons or organizations that can affect or can be affected by information security or business continuity management (interested parties), and (2) all related legal, regulatory and other requirements, with Legal Department support.

The Top Management Representative, with support from the Legal department, is responsible for identifying all the contractual requirements around information security.

The Top Management Representative will define who will be responsible for compliance with each individual requirement, and which interested parties are to be notified when changes occur.

Contractual requirements are communicated and addressed to the responsible parties according to the procedures related to the service or development.

The Top Management Representative must list all requirements, interested parties, and responsible persons in the "List of legal, regulatory and other requirements," and publish that List in the Stefanini Portal or other appropriate location.

Every employee in Stefanini must notify the Top Management Representative if he/she comes across any new legal, regulatory, contractual or other requirement that might be relevant to information security and business continuity management.

3.2. Reviewing and evaluation

The Top Management Representative is responsible for reviewing the List of legal, regulatory and other requirements, with Legal Department support, semiannually, and update as necessary. The Top Management Representative will notify all relevant interested parties upon each update.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 259

The Top Management Representative is responsible for evaluating the compliance of ISMS with relevant legal, regulatory and contractual requirements at least once a year. External parties may be used to assist in compliance.

4. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Control for record protection	Retention time
List of legal, regulatory and other requirements (in electronic form)	Stefanini's intranet or portal or other appropriate location	Top Management Representative	Only Top Management Representative is authorized to edit data	Old versions of the List are archived for 1 year

5. Document management

The owner of this document is the Top Management Representative, who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria must be considered:

- Results of management review
- Audits results

A current version of this document is available to all staff and under version control on the corporate document control system.

6. Appendices

- Not applicable

7. Change history

Date	Version	Created by	Description of change
22-JAN-2014	1.0	Rodrigo Ricci	Document creation
16-SEP-2016	2.0	Elaine Pinheiro	Changed period of review

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 260

stefanini
POWERING YOUR BUSINESS

DOCUMENT AND RECORD CONTROL PROCEDURE

Information Security Management System



Code:	ISMS-006
Version:	3.1
Date of version:	11-AUG-2015
Updated by:	Matthew Engler
Approved by:	Washington Souza
Confidentiality level:	Internal Use

Table of contents

1. PURPOSE, SCOPE AND USERS 3
2. REFERENCE DOCUMENTS 3
3. DESCRIPTION 3
3.1 CONTROL OF INTERNAL DOCUMENTS 3
3.1.1 DOCUMENT FORMATTING 3
3.1.2 DOCUMENT APPROVAL 3
3.2 DOCUMENT UPDATES 4
3.3 RECORDS CONTROL 4
3.4 DOCUMENTS OF EXTERNAL ORIGIN 4
4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 5
5. DOCUMENT MANAGEMENT 5
6. APPENDICES 5
7. CHANGE HISTORY 5

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 262

1. Purpose, scope and users

The purpose of this procedure is to ensure control over creation, approval, distribution, usage and updates of documents and records (also called: documented information) used in the Information Security Management System (ISMS).

This procedure applies to all documents and records related to the ISMS, regardless of whether the documents and records were created inside Stefanini or whether they are of external origin.

This policy applies to Stefanini Employees, sub-contractors, consultants, business associates, and other workers at Stefanini (collectively “User(s)”) inside the scope of the ISMS.

2. Reference documents

Documents associated or linked tare listed below:

- ISO/IEC 27001 standard, 7.5.2, 7.5.3, A.18.1.3, A.18.2.2
- ISMS-001 Policy, Information Security
- Retetion Policy

3. Description

3.1 Control of internal documents

Internal documents are all documents created inside the organization.

3.1.1 Document formatting

For the ISMS standard operating policies and procedures, the document front page contains organization name, confidentiality level current version and date of document. The footer contains document name and number of pages.

Every document must also define its users.

3.1.2 Document approval

All documents, regardless of whether they are new documents or new versions of existing documents, must be approved electronically by the responsible parties involved in the activities. Those responsible are defined by the Top Management Representative, taking into account the process described in the document, the involvement of people with this activity and its authority.

Document Administrators will be able to perform administrative changes without going through formal approval. Administrative changes do not affect the purpose/intent, responsibilities, or process steps of the document. Some examples include change in author, owner, typos, spelling and grammar errors. Request for these types of changes must be documented in a SSD ticket to the Quality support group. Changes will be recorded in the Change History table of the eDoc document profile.

The approval workflow is defined and recorded within the electronic system.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 263

3.2 Document updates

The person listed as document owner has the responsibility for updating the document as needed. Updates are performed in line with the frequency defined for each document. Documents must be reviewed at least once a year.

All changes to the document must be made using "Track changes," making visible only the revisions to the previous version, and must be briefly described in the "Change History" table; if Track changes option is unavailable, or if the changes are too numerous, then the Track changes option is not used.

Each document should preferably have a "Change History" table used to record every change made to the document.

The approval workflow is defined and recorded within the electronic system.

3.3 Records control

Each internal document in the ISMS must define how records resulting from the use of such a document should be managed, i.e. it must specify the following: (1) record title, (2) storage location, (3) person responsible for storage, (4) controls for record protection, and (5) retention time.

Employees of the organization may access stored records only after obtaining permission from the person designated as the person responsible for storing individual records. If the sensitivity of certain records is such that permission for access must be obtained from a different person, this must be stated in the concerned internal document in the chapter describing records control.

Access and retrieval rights for records are determined by the owner of individual records. The owner or designated professional is responsible for destroying all records of which the retention time has expired.

3.4 Documents of external origin

Each external document, which is necessary for the planning and operation of the ISMS, must be recorded in the ISMS Portal and controlled by the systematic control of documents. Each external document, which is necessary for the execution of the service, will be controlled according to the methodology of the service.

Mail and courier parcels will be received through either, a designated Administrative Area (e.g. front desk reception) or through a Receiving Area (e.g. loading dock). For those items received through an Administrative Area (typically mail, small packages), the receiver will classify documents according to the Information Classification policy. For any document classified as Public, it may be placed in an unsecured mail area (e.g. copy room). For any document classified as Confidential or above, the mail will be placed in a secured mail area, which may include the user's workstation or other isolated mail area with limited access. For those items received through a Receiving Area (typically larger packages, equipment), the receiver will consider the asset as Confidential. The receiver will record the package information within a standard system and follow appropriate Asset procedures (where defined). Packages will be either, delivered to the user's workstation, or remain in a secured area for the user to pick-up.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 264

4. Managing records kept on the basis of this document

- Not Applicable

5. Document management

The owner of this document is the Top Management Representative, who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

- number of obsolete or out-of-date documents
- number of documents that were not distributed to intended employees
- number of documents for which no record is kept or which are not appropriately stored

A current version of this document is available to all staff and under version control on the corporate document control system.

6. Appendices

- Not applicable

7. Change history

Date	Version	Created by	Description of change
11-DEC-2013	1.0	Larissa Longo	Document creation
22-JAN-2014	2.0	Larissa Longo	Included use of electronic system to control and record the workflow on document approval
22-SEP-2014	3.0	Matt Engler	Removed reference to incoming mail register as a record.
11-AUG-2015	3.1	Matt Engler	Removed reference to video/audio documents/ Added yearly review requirement.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 265

stefanini
POWERING YOUR BUSINESS

MANAGEMENT REVIEW PROCEDURE

Information Security Management System



Code:	ISMS-007
Version:	2.0
Date of version:	24-AUG-2020
Created by:	Matthew Engler
Approved by:	Washington Souza
Confidentiality level:	Internal Use

Table of contents

1. PURPOSE, SCOPE AND USERS 3
2. REFERENCE DOCUMENTS 3
3. DESCRIPTION 3
3.1 MANAGEMENT REVIEW 3
3.1.1 PREPARATION OF THE REVIEW 3
3.1.2 INPUT AND OUTPUT 3
3.1.3 MANAGEMENT REVIEW REPORT 4
4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 4
5. DOCUMENT MANAGEMENT 4
6. APPENDICES 5
7. CHANGE HISTORY 5

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 267

1. Purpose, scope and users

The purpose of this procedure is to describe how to document information for the management review, the frequency of the review and the outputs of the management review.

Users of this document are members of Top Management of Stefanini, as well as internal auditors.

2. Reference documents

Documents associated or linked are listed below:

- ISO/IEC 27001 standard, 9.3
- ISMS-001 Policy, Information Security
- ISMS-009 Procedure, Corrective and preventive actions
- Targets and objectives

3. Description

3.1 Management review

3.1.1 Preparation of the review

Top Management nominates a representative for all management activities of the ISMS but does not delegate their responsibilities and commitment on ISMS.

The Top Management Representative, or their designated proxy, is responsible for gathering all the information necessary from the sites under the ISMS.

The information can include a previous review from the sites in order to make a consolidated and complete management review of the ISMS.

Management reviews are performed at least once a year.

3.1.2 Input and output

Inputs to the management review shall include:

- Results of ISMS audits and management reviews;
- Feedback from interested parties;
- Techniques, products or procedures that may be used in the organization to improve the performance and effectiveness of the ISMS;
- Status of preventive and corrective actions;
- Vulnerabilities or threats not adequately addressed in the analyzes / evaluations of previous risk;
- Efficiency results of measurements;

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 268

- Follow-up actions from previous management reviews;
- Any changes that may affect the ISMS, and
- Recommendations for improvement.

The output from the management review shall include any decisions and actions related to:

- Improving the effectiveness of the ISMS.
- Update of the analysis / risk assessment and risk treatment plan.
- Modification of procedures and controls that affect the security of information, as necessary, to respond to internal or external events that may impact on the ISMS, including changes:
- Business requirements;
- Requirements for information security;
- Business processes that affect the requirements of existing business;
- Contractual obligations, and
- Legal or regulatory requirements;
- Levels of risk and / or risk acceptance criteria.
- The need for resources.
- Improvement of the effectiveness of controls is being measured.

3.1.3 Management review report

The Top Management Representative, or their designated proxy, shall record the discussions, subjects and decisions made during the review.

For Stefanini Colombia, the procedure to use is Review by Management PC-RD-01.

The actions defined are implemented according to the *ISMS-009 Procedure, Corrective and preventive actions*.

For Stefanini Colombia, the procedure to use is Corrective Actions PC-MM-02 and the registration tool is Corrective Actions FR-MM-05.

4. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
Management review report	Stefanini´s SharePoint	Top Management Representative	Only Top Management Representative has the right to make entries into and changes.	Reports are stored for a period of 2 years

5. Document management

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 269

The owner of this document is the Top Management Representative, who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria must be considered:

- Results of the objectives
- Audits results

A current version of this document is available to all staff and under version control on the corporate document control system.

6. Appendices

- Not applicable

7. Change history

Date	Version	Created by	Description of change
22-JAN-2014	1.0	Larissa Longo	Document creation
11-AUG-2015	1.1	Matthew Engler	Added the ability to designate an additional person to handle the management review.
24-AUG-2020	2.0	Licsileth Palma	The use of procedures PC-RD-01, PC-MM-02 and the FR-MM-05 format - included for Colombia

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 270

stefanini
POWERING YOUR BUSINESS

INTERNAL AUDIT PROCEDURE

Information Security Management System



Code:	ISMS-008
Version:	3.0
Date of version:	28-AUG-2020
Created by:	Matthew Engler
Approved by:	Washington Souza
Confidentiality level:	Internal Use

Table of contents

1. PURPOSE, SCOPE AND USERS 3
2. REFERENCE DOCUMENTS 3
3. DESCRIPTION 3
3.1 INTERNAL AUDIT 3
3.1.1 PURPOSE OF INTERNAL AUDIT 3
3.1.2 INTERNAL AUDIT PLANNING 3
3.1.3 APPOINTING INTERNAL AUDITORS 4
3.1.4 CONDUCTING INDIVIDUAL INTERNAL AUDITS 4
3.2 CONDUCTING A TECHNICAL AUDIT 7
4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 8
5. DOCUMENT MANAGEMENT 8
6. APPENDICES ..... ERROR! BOOKMARK NOT DEFINED.
7. CHANGE HISTORY ..... ERROR! BOOKMARK NOT DEFINED.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 272

1. Purpose, scope and users

The purpose of this procedure is to describe all audit-related activities – writing the audit program, selecting an auditor, conducting individual audits and reporting.

Users of this document are members of Top management of Stefanini, as well as internal auditors.

2. Reference documents

Documents associated or linked are listed below:

- ISO/IEC 27001 standard, 9.2, A.12.7.1, A.18.2.1, A.18.2.3
- ISMS-001 Policy, Information Security
- ISMS-009 Procedure, Corrective and preventive actions

3. Description

3.1 Internal audit

3.1.1 Purpose of internal audit

The purpose of an internal audit is to determine whether procedures, controls, processes, arrangements and other activities within the ISMS are in line with ISO 27001 standard, applicable regulations, and the organization's internal documentation, whether they are effectively implemented and maintained and whether they meet policy requirements and objectives.

Note: In Stefanini Colombia, the procedure to use is **Plan and Conduct of Audits PC-AU-01.**

3.1.2 Internal audit planning

The Top Management Representative approves an annual program for internal audits.

One or more internal audits should be conducted in the course of one year, ensuring cumulative coverage of the entire ISMS scope. Internal audits are planned based on risk assessment, as well as results of previous audits; they are usually conducted before a management review.

The Annual Internal Audit Program has to contain the following information about each individual internal audit:

- period of the audit (specifying dates, or month in which the audit is planned)
- scope of the audit (departments, processes, clauses of the standard, etc.)
- audit criteria (standards, legislation and regulations, internal documentation, corporate standards, and/or contractual obligations)
- who will be conducting the audit (if there is more than one auditor, specify the Lead ISMS Auditor)

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 273

Conducted audits must be recorded in the Annual Internal Audit Program.

3.1.3 Appointing internal auditors

The Top Management Representative shall appoint internal auditors.

An internal auditor may be someone from the organization or a person outside the organization.

ISMS Auditors shall be qualified, based upon one of the following criteria:

- ISO 27001 Lead Auditor Certification:
  - International Register of Certificated Auditors (IRCA)
  - PECB
- Security Professional Certification:
  - Information Systems Audit and Control Association® (ISACA)
    - Certified Information Systems Auditor (CISA)
    - Certified Information Security Manager (CISM)
- Accredited ISO 27001 Auditor Courses
  - For example: https://training.advisera.com/course/iso-27001-lead-auditor-course/
- Approved through Auditor Competence Process (Appendix 6)
- Auditor for another Management System / ISO Standard (e.g. ISO 9001) with knowledge of ISO/IEC 27001 standard and how information and communication technologies function to the extent that he/she is familiar with the purpose of individual systems as well as the impacts on security processes.

Internal auditors must be selected in such a way as to ensure objectivity and impartiality, i.e. to avoid conflict of interest, because auditors are not allowed to audit their own work.

3.1.4 Conducting individual internal audits

Persons responsible for individual internal audits are identified in the Annual Internal Audit Program. If an audit is conducted by a team consisting of several auditors, the person responsible for the audit is the one identified as Audit Team Leader.

The following must be taken into consideration during an internal audit:

- criteria laid down in the Annual Internal Audit Program
- results of previous internal or external audits
- results of risk assessment, controls implementation, business impact analysis, etc.
- Internal audit checklist

The following must be documented as internal audit results:

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 274

- Internal Audit Report – it must be sent to Top Management Representative
- possible corrective actions must be documented in the Corrective Action Form, as required by the *ISMS-009 Procedure, Corrective and preventive actions*.

3.1.5 Evidence Guidelines

1.1.5.1 Concepts Relating to Audit Evidence

Audit evidence provides the foundation for the Internal Audit report. Therefore, it is important that the ISMS auditors understand the nature of evidence and its critical role in the entire audit process. Audit evidence should be as accurate and complete as possible. The more important characteristics associated with good evidence are:

- **Relevance** - refers to the relationship of evidence to its use. The information used to prove or disprove an issue is relevant if it has a logical, pertinent and sensible relationship to the particular issue that is the subject of the audit. Information that is irrelevant should not be included as evidence or included in audit reports.
    - Questions that test the relevancy of evidence include the following:
        - Is the evidence related to such factors as background, condition, criteria, effect or cause?
        - Does the evidence make an asserted finding, conclusion or recommendation more believable?
- **Reliability** - refers to the appropriateness, soundness, trustworthiness or credibility of the sources of information and the techniques used to obtain the information. Generally evidence is more reliable if is obtained or developed from:
    - A credible independent source other than from the person being audited.
    - A good system of internal controls rather than that obtained from a source where such control is weak or unsatisfactory.
    - Direct physical examination, observation, computation, and inspection rather than indirectly.
    - Documented sources rather than verbal sources and original documents rather than copies.
    - Discussion evidence obtained under conditions where the person being audited may speak freely rather than evidence obtained under compromising conditions (e.g., where the persons may be intimidated).
- **Sufficiency** - relates to quantity. There should be enough factual and convincing evidence to evaluate so that a reasonably informed and unbiased person would agree with the ISMS auditor's findings and conclusions. Determining the sufficiency of evidence requires professional judgment. When considering the adequacy of evidence, the auditor should keep in mind that:
    - The audit is seeking reasonable, but not absolute, conclusions.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 275

- Incomplete data may result in inability to reach reasonable conclusions.
- Examination of extensive evidence may be uneconomical, inefficient and ineffective.
- Evidence should be reasonably representative of the population being reviewed or addressed.

1.1.5.2 Methods of obtaining evidence

Audit evidence can be collected using a variety of tools and techniques. Different tools and techniques have various strengths and weaknesses. For example, one may require a high degree of technical skill while another a high degree of interpersonal skill; one may be expensive but reliable, another inexpensive but less reliable. The Lead ISMS Auditor should consider the most appropriate as well as the most practical and cost-efficient method for collecting relevant information. It may include:

- **Interviews –** Interviews are used to gather verbal evidence and opinions. Interviews can help to define the issues, furnish evidence to support audit findings, and clarify audit observations and recommendations. Adequate preparation and good skills are needed to use interviews effectively in building or confirming audit evidence.
- **Audit Testing** - Testing implies the evaluation or measurement of transactions or processes to determine their qualities or characteristics. The particular transaction or element to be tested is put on 'trial'. A common audit test is a compliance test. Compliance tests are typically designed to assess the adequacy and effectiveness of specific controls.
- **Sampling** - It is rarely feasible to test every item within an entire population because of prohibitive costs and the time required. Instead, ISMS auditors should select a sample of items from within the population and conduct such tests as are necessary on the items contained in the sample to make conclusions about or determine the parameters and characteristics (attributes) of the whole population. The objective of sampling is to gather data based on tests of a limited number of people, things, processes, transactions, documents, etc. that represent the larger group or population. In order to serve a useful purpose, sampling needs to be properly planned to ensure that the sample in fact represents the population that is the subject of the audit. Where a sample does not effectively represent the population, then the conclusions drawn from the tests conducted will only represent or relate to the items that are tested and not the population.
- **Inspection** - Inspection consists of confirming the existence or status of records, documents or physical assets. Inspection of physical assets provides highly reliable evidence of their existence or condition. Inspection of records could confirm the existence of source documents for data entry, e.g. program participant questionnaires or evaluations.
- **Observation** - Like inspection, observation entails personally verifying or attesting to a process or procedure, e.g. the application of controls by employees or managers. Many internal control can only be evaluated by seeing someone perform them. Whenever possible, two or more auditors should be present to make observations in order to provide additional support to the observations.

In general, evidence accumulated from different sources and of different types is strongest. The determination of when it is necessary to gather corroborating evidence from different sources or of a

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 276

different nature is a matter of professional judgment. Factors that may be taken into consideration when deciding whether or not to seek additional evidence include:

- Is there a high degree of consistency among the evidence already collected (i.e. the lack of contradictory evidence)? If there is no contradiction, the need for additional evidence is decreased; if not, the need is increased.
- Is there a high degree of risk, significance or sensitivity associated with the matter to be reported? If so, additional evidence may reinforce the internal auditor's conclusion; if not, existing evidence may be sufficient to gain acceptance of the conclusion.
- Is the cost of obtaining additional evidence worth the benefits to be obtained in terms of supporting the finding? If it is costly, additional effort should be carefully considered. Otherwise, proceed.

3.2 Conducting a technical audit

Top Management Representative must appoint a person with sufficient skills to review the information systems for compliance with the organization's information security policies and standards. Audit records will be maintained and deficiencies will be handled through the Corrective Action Procedure. Technical audits should follow the evidence guidelines documented in 3.1.5. If penetration tests or vulnerability assessments are used, caution will be exercised as such activities could lead to a compromise of the security of the system

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 277

4. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
Annual Internal Audit Program (in electronic form)	Stefanini´s portal	Top Management Representative	Only Top Management Representative has the right to make entries into and changes to the Annual Internal Audit program.	Programs are stored for a period of 3 years
Internal Audit Report (in electronic form) or Internal Audit Checklist (filled form during the internal audit)	Stefanini´s portal	Top Management Representative	Reports are stored in read-only versions	Reports / checklists are stored for a period of 3 years
Internal Auditor Competence	Stefanini's portal	Top Management Representative	Only Top Management Representative has the right to make entries into and changes to the document.	Stored for as long as the auditor is active.

Only the Top Management Representative can grant other employees the right to access the Annual Internal Audit Program, the Internal Audit Report and the Internal Audit Checklist.

5. Document management

The owner of this document is the Top Management Representative, who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria must be considered:

- Results of the objectives
- Audits results

A current version of this document is available to all staff and under version control on the corporate document control system.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 278

6. Appendices – Auditor Competence Process

6.1. Assess Existing Competence Levels

In order to assess the current competence levels of individuals that are to fulfil specific auditor roles, a questionnaire approach is used. The people that are to take each role are first identified.

An appropriate questionnaire is then created for each role that includes all of the competences that have been identified as being required for that role. The required levels of competence should not be included within the questionnaire. All relevant staff are then asked to complete the questionnaire as objectively as possible using the competence level definitions shown in the table below.

Skill Level	Summary	Guidance
0	None	You have no knowledge or experience in this area and it is not part of your role.
1	Low	The competence area is used infrequently and is largely based upon observation of how others do it, with little understanding of why specific tasks are performed. Perhaps the competence area has only been practised for a relatively short period of time and is not seen as part of the individual's job role. No formal training has been given. A general awareness.
2	Medium	The competence area is regularly practiced as part of the job role and this has probably been the case for a long enough period for the individual to feel comfortable doing it (more than a year). Informal and in some cases formal training may have been received and there is an understanding of the principles behind the skill. The individual feels competent in this area.
3	High	The competence area is seen as a particular strength and is backed by significant training, qualifications and experience over a lengthy period of time (probably more than 3 years). The principles are fully understood and the individual keeps up to date with developments in this area. They may have trained others and been responsible for developing processes and procedures and been involved in several projects which have made use of the skill.
4	Expert	The individual is externally recognised as a subject matter expert who contributes to developments in this area and may be involved in industry events such as presenting at conferences and seminars. He/she is held in high esteem by suppliers and customers and may assist in developing and testing new products and services.

Table 1 - Competence level definitions

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 279

Individuals' responses should then be validated by an existing ISMS auditors or top management representative, depending on the nature of the individual's role. This should ensure an increased level of consistency in the responses, as some people are more likely to over- or under-estimate their competency levels than others. Where there is disagreement about a level of competence, the situation should be discussed with the relevant individual to understand the reason for the discrepancy. If there is continued disagreement, a decision should be taken by the top management representative about which level should be used.

6.2. Evaluate Effectiveness

The approved actions identified to develop competence in specific individuals should be reviewed for effectiveness both as part of employee performance reviews and regular management reviews of ISO 27001:2013 compliance.

Once a development action has been completed, a re-assessment should be carried out to check that it has resulted in the individual possessing the required level of competence. If this is not the case, the reasons for this should be established and, if necessary, further actions identified to achieve the required result.

Appropriate documented evidence should be retained of all actions carried out. This may include training records, mentoring logs or third party contracts.

6.3. Required Competences by Role

The following lists are intended to act as a starting point for the competences required for each of the roles related to ISO 27001:2013 Auditing.

6.3.1. ISMS Auditor

Competence	Required Level
General Understanding of ISO Management Systems	2
Knowledge of Auditing Practices	2
Specific to ISO 27001:2013 – Stefanini – Knowledge of the following:	
Context of Organization; Scope	1
ISMS Policy	1
ISMS Roles / Responsibilities	1
Document Control	2
Corrective Actions	2
Management Review	1
Knowledge of the ISO 27002:2013 – Controls: **Note: Auditor may have knowledge in specific areas, only, and audit as such.**	
Information Security Policies	2
Organization of Information Security	2
Human Resources Security	2
Asset Management	2

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 280

Competence	Required Level
Access Control	2
Cryptography	2
Physical and Environmental Security	2
Operations Security	2
Communications Security	2
Sys Acquisition, Dev and Maintenance	2
Supplier Relationships	2
Information Security Incident Management	2
Information Security Business Continuity Management	2
Compliance	2

7. Change history

Date	Version	Created by	Description of change
22-JAN-2014	1.0	Rodrigo Ricci	Document creation
1-AUG-2019	2.0	Matthew Engler	Added additional explanation around auditor requirements; Competence; and audit plans
28-AUG-2020	3.0	Licsileth Palma	Included for Colombia the procedure to be used - Plan and Conduct of Audits PC-AU-01.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 281

CORRECTIVE AND PREVENTIVE ACTIONS PROCEDURE

Information Security Management System



Code:	ISMS-009
Version:	3.0
Date of version:	24-AUG-2020
Created by:	Licsileth Palma
Approved by:	Washington Souza
Confidentiality level:	Internal Use

Table of contents

1. PURPOSE, SCOPE AND USERS 3
2. REFERENCE DOCUMENTS 3
3. DESCRIPTION 3
3.1. DEFINITION 3
3.2. SOURCE OF ACTIONS 3
3.3. ROOT CAUSE DETERMINATION 4
3.4. ACTION PLAN 4
3.5. ACTIONS FOLLOW-UP 4
3.6. ACTIONS EFFECTIVENESS 4
4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 4
5. DOCUMENT MANAGEMENT 4
6. APPENDICES 5
7. CHANGE HISTORY 5

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 283

1. Purpose, scope and users

The purpose of this procedure is to establish how we implemented Corrective, Preventive Actions and Enhancements on Stefanini´s ISMS, to ensure its continuing suitability, adequacy and effectiveness.

Users of this document are members of Top management of Stefanini, as well as internal auditors.

2. Reference documents

Documents associated or linked are listed below:

- ISO/IEC 27001 standard, 10.1
- ISMS-001 Policy, Information Security
- ISMS-007 Procedure, Management review
- ISMS-023 Procedure, Incident Management
- Strategic objectives
- Internal Audit Report

3. Description

3.1. Definition

Non-conformity: non-compliance with a specified requirement, control, procedure or policy;

Corrective action: action taken on the causes of non-compliance with the objective to minimize, neutralize or eliminate the effects in order to avoid their recurrence;

Immediate action: action taken to solve the problem effects.

Preventive action: action taken on the causes of potential nonconformities or events in order to minimize, neutralize or eliminate the effects in order to avoid their occurrence.

Improvement action: action taken to make a control, activity or process more effective or efficient.

3.2. Source of actions

The source of actions can be:

- Management review;
- Strategic objectives results;
- Internal and external audits results;
- Incidents and events report;
- Simulations results on continuity plan;

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 284

- Effectiveness indicators results.

3.3. Root cause determination

The person responsible to take action must determine the root cause of the problem, real or potential, and make sure that acting on this root cause, the problem will not happen again. Various root cause methods may be used, like 5 Why or Fishbone Diagram.

3.4. Action plan

Immediate action is used when possible to block the effects of the problem. It is not corrective action.

Actions must be defined, with due dates and responsible, to solve the root cause.

The corrective plan is addressed to the one responsible for the actions.

3.5. Actions follow-up

The action owner follows the dates and the actions implementation making sure that they will happen on time.

Top Management Representative (corporate, regional or local) or Internal Auditor can follow the actions and ask for evidence of the implementation.

3.6. Actions effectiveness

The Top Management Representative (corporate, regional or local), Internal Auditor, or Information Security Manager checks the actions effectiveness to make sure that the problem is solved and the cause eliminated. Evidence on this checking is noted in the Corrective Action record.

Note: For Stefanini Colombia, the procedure to use is **Acciones Correctivas PC-MM-02** and the record tool is **Acciones Correctivas FR-MM-05**.

4. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
Corrective action Report	Corrective action tool	Corrective Action Owner	Refer to Backup procedure	3 years

5. Document management

The owner of this document is the Top Management Representative, who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria must be considered:

- Results of the objectives
- Audits results

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 285

A current version of this document is available to all staff and under version control on the corporate document control system.

6. Appendices

- Not applicable

7. Change history

Date	Version	Created by	Description of change
22-JAN-2014	1.0	Rodrigo Ricci	Document creation
05-NOV-2019	2.0	Elaine Pinheiro	Improvement actions were included, the responsibilities of the senior management representative were clarified.
24-AUG-2020	3.0	Licsileth Palma	The use of the PC-MM-02 procedure and the FR-MM-05 registration tool are included for Colombia.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 286

ACCEPTABLE USE POLICY

Information Security Management System



Code:	ISMS-010
Version:	4.0
Date of version:	24-AUG-2020
Created by:	Licsileth Palma
Approved by:	Washington Souza
Confidentiality level:	Internal Use

Table of contents

1. PURPOSE, SCOPE AND USERS 3

2. REFERENCE DOCUMENTS 3

3. DESCRIPTION 3

3.1 ACCEPTABLE USE OF INFORMATION ASSETS 3

3.1.1 DEFINITIONS 3

3.1.2 ACCEPTABLE USE 4

3.1.3 RESPONSIBILITY FOR ASSETS 4

3.1.4 PROHIBITED ACTIVITIES 4

3.1.5 TAKING ASSETS OFF-SITE 5

3.1.6 RETURN OF ASSETS UPON TERMINATION OF CONTRACT 6

3.2 BACKUP PROCEDURE 6

3.3 ANTIVIRUS PROTECTION 6

3.4 AUTHORIZATIONS FOR INFORMATION SYSTEM USE 6

3.5 USER ACCOUNT RESPONSIBILITIES 6

3.6 PASSWORD RESPONSIBILITIES 7

3.7 CLEAR DESK AND CLEAR SCREEN POLICY 7

3.8 INTERNET USE 7

3.9 E-MAIL AND OTHER MESSAGE EXCHANGE METHODS 7

3.9.1 PROHIBITED EMAIL AND COMMUNICATIONS ACTIVITIES 8

3.9.2 BLOGGING / SOCIAL NETWORKING 8

3.10 COPYRIGHT 9

3.11 MOBILE COMPUTING 9

3.12 MONITORING THE USE OF INFORMATION AND COMMUNICATION SYSTEMS 9

3.13 INCIDENTS 9

4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 10

5. DOCUMENT MANAGEMENT 10

6. APPENDICES 10

7. CHANGE HISTORY 11

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 288

1. Purpose, scope and users

The purpose of this document is to define clear rules for the use of the information system and other information assets in Stefanini.

This policy applies to Stefanini Employees, sub-contractors, consultants, business associates, and other workers at Stefanini, including all personnel affiliated with third parties and subsidiaries on the Stefanini infrastructure (collectively “User(s)”).

2. Reference documents

Documents associated or linked are listed below:

- ISO/IEC 27001 standard, A.6.2.1, A.6.2.2, A.8.1.2, A.8.1.3, A.8.1.4, A.8.2.3, A.9.3.1, A.11.2.5, A.11.2.6, A.11.2.8, A.11.2.9, A.12.2.1, A.12.3.1, A.12.5.1, A.12.6.2, A.13.2.3, A.18.1.2
- ISMS-001 Policy, Information Security
- ISMS-022 Policy, Clear desk and clear screen
- ISMS-023 Procedure, Incident management
- ISMS-027 Policy, Information Transfer
- ISMS-028 Policy, Information Classification
- ISMS-042 Policy, Removable Storage Media
- ISMS-043 Policy, Account and Password
- ISMS-044 Policy, Use of Cryptographic Controls
- ISMS-047 Policy, Mobile Device and Teleworking
- ISMS-069SH Procedure Off-Boarding of Personnel

3. Description

3.1 Acceptable use of information assets

3.1.1 Definitions

Information system – includes all servers and clients, network infrastructure, system and application software, data, and other computer subsystems and components which are owned or used by the organization or which are under the organization's responsibility. The use of an information system also includes the use of all internal or external services, such as Internet access, e-mail, etc.

Information assets – in the context of this Policy, the term *information assets* is applied to information systems and other information/equipment including paper documents, mobile phones, portable computers, data storage media, etc.

Sensitive Information - All information classified as "Internal use," "Confidential" and "Restricted" as specified in the *ISMS-028 Policy, Information Classification*.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 289

3.1.2 Acceptable use

Information assets may be used only for business needs with the purpose of executing organization-related tasks. Using Stefanini resources for personal business or for other unauthorized commercial gain is prohibited.

3.1.3 Responsibility for assets

Each information asset has an owner designated in the Inventory of Assets. The asset owner is accountable for the confidentiality, integrity and availability of information in the asset in question.

3.1.4 Prohibited activities

The following activities are, in general, prohibited. Users may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may need to disable the network access of a host if that host is disrupting production services). It is prohibited to use information assets in a manner that unnecessarily takes up capacity, weakens the performance of the information system or poses a security threat.

Under no circumstances is a User authorized to engage in any activity that is illegal under local, state, federal, or international law while using Stefanini-owned resources.

The following lists are not intended to be exhaustive, but are provided as a framework and guidelines for activities that fall into the category of unacceptable use. If for any reasons there are questions as to what is acceptable and unacceptable use, please contact Human Resource or the Information Security Manager. It is also prohibited:

- Physically connecting an unauthorized computing device to the Stefanini network. The Infrastructure and Support department in cooperation with the Information Security Manager must approve all devices before they are connected to the network.
- Storing or transporting Stefanini Confidential or Restricted Information on personal USB or personal portable storage devices.
- Attempting to bypass protections on the use of peripheral devices such as modems, memory cards or other devices for storing and reading data (e.g. USB flash drives). Please refer to *ISMS-042 Policy, Removable Storage Media* for additional information.
- Installing software on a local computer without the explicit permission of Information Security Manager.
- Using Java applications, Active X controls and other mobile code, except where authorized through completed Service Request or as required by a Stefanini authorized application.
- Downloading program code from external media.
- Using cryptographic tools (encryption) on a local computer, except in the cases specified in the *ISMS-028 Policy, Information Classification* and in accordance with *ISMS-044 Policy, Use of Cryptographic Controls.*
- Downloading, copying, or storing files (video clips, graphics, mp3s, or programs) for personal use on network resources.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 290

- Storing any Stefanini Restricted Information on the hard drive of a desktop/laptop intended for multiple users, including files downloaded from the Internet.
    - **NOTE**: *Only files saved in the designated network folders are backed up daily. If you store files on any hard drive, you do so at your own risk.*
- Intentional introduction of malicious programs into the network or server (e.g., viruses, worms, malware, Trojan horses, email bombs).
- Using a Stefanini computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any Stefanini account.
- Posting any material that is obscene, defamatory, profane, libelous, threatening, harassing, abusive, hateful or embarrassing to another person or any other person or entity on Instant Message programs, chat rooms and blogs. This includes, but is not limited to, comments regarding Stefanini, Stefanini employees, Stefanini's partners and Stefanini's competitors.
- Making statements about warranty of products or services, expressly or implied, unless it is a part of normal job duties and has been approved by Stefanini's Legal Department.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the User is not an intended recipient or logging into a server or account that the User is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Port scanning or security scanning is expressly prohibited by end Users.
- Executing any form of network monitoring that intercepts data not intended for the User's host, unless this activity is a part of the User's normal job/duty and has been approved by the Information Security Manager.
- Circumventing user authentication or security of any host, network, or account.
- Interfering with or denying service to any user other than the User's host (e.g., denial of service attack).
- Using any program/script/command or sending messages of any kind with the intent to interfere with or disable a user's terminal session through any means locally or through the Internet/Intranet/Extranet.
- Using any remote desktop access to another system for any means without expressed consent from the end user or authorization from the Information Security Manager. This includes remote desktop support, file shares, email and other areas where confidential information may be obtained.
- Providing information about, or lists of, Stefanini Users to parties outside Stefanini.

3.1.5 Taking assets off-site

Equipment, information or software, regardless of its form or storage medium, may not be taken off-site without proper documentation completed. Where applicable, additional confidentiality statements may be required.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 291

As long as said assets are outside the organization, they have to be controlled by the person who was granted permission for their removal.

3.1.6 Return of assets upon termination of contract

Upon termination of an employment contract or other contract on the basis of which various equipment, software or information in electronic or paper form is used, the user must return all such information assets to the Infrastructure and Support Department, or other appropriate authority (e.g. their manager). Refer to ISMS-069 Off-boarding procedure.

Note: For Colombia, refer to Instructivo IN-SI-01 Instructivo de Off-Boarding.

3.2 Backup procedure

The user must backup changes to all sensitive information stored on his/her computer at least once per day. This may include backing up to a network resource. Network resources are backed up as part of the enterprise backup procedures.

3.3 Antivirus protection

All PCs utilized by Users who are connected to the Stefanini Internet/Intranet/Extranet, whether owned by the User or Stefanini, must continually execute approved virus-scanning software with a current virus database unless overridden by departmental or group policy.

Mobile devices such as phone or tablet devices connected to the Stefanini network should maintain virus-scanning software, if available.

3.4 Authorizations for information system use

Users of the information system may only access those information system assets for which they have been explicitly authorized by the asset owner. Stefanini Employees will be required to sign a contract and/or confidentiality agreement and it will be stored with the appropriate organization (e.g. Human Resources' personnel records).

Users may use the information system only for purposes for which they have been authorized, i.e. for which they have been granted access rights.

Users must not take part in activities, which may be used to bypass information system security controls.

Personal computers may only be used to connect to the Stefanini network in the following ways:

- From outside the company using approved VPN Technology authorized in the Infrastructure and Support Department or the Information Security Manager.
- From within a Stefanini facility using Visitor access on the guest wireless network. Use of Visitor access on the guest wireless is subject to monitoring. Personal computers may not be connected physically to the Stefanini network under any circumstances.

3.5 User account responsibilities

The user must not, directly or indirectly, allows another person to use his/her access rights, i.e. username, and must not use another person's username and/or password. Sharing or allowing others to use your Stefanini issued Photo ID, Access Badge, Keys or any other device which grants access to a Stefanini facility or network resources is prohibited. The use of group user names is forbidden.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 292

The owner of the user account is its user, who is responsible for its use, and all transactions performed through this user account.

3.6 Password responsibilities

Users must apply good security practices when selecting and using passwords, according to the accounts and passwords policy. Users must keep passwords secure and must not share accounts. Revealing account passwords to others or allowing the use of accounts by others is prohibited. This includes family and other household members when work is being done at home.

Authorized Users are responsible for the security of their passwords and accounts. Users' passwords must be changed in accordance with *ISMS-043 Policy, Account and Password*.

All desktop and portable computers will be configured to auto-lock within 15 minutes of inactivity.

3.7 Clear desk and clear screen policy

Apply the *ISMS-022 Policy, Clear desk and clear screen*

3.8 Internet use

The Internet may only be accessed through the organization's local network with appropriate infrastructure and firewall protection. Attempts to bypass Internet protections or connecting any unauthorized modems, wireless networks or other devices to create a direct Internet access point is forbidden. All wireless connection points must be authorized by the Infrastructure and Support Department.

Access to certain Internet pages may be blocked for individual users, groups of users or all users at the organization. If access to some web pages are blocked, the user may submit a Request via the Service Request process for authorization to access such pages. The user must not try to bypass such restriction autonomously.

The user must regard information received through unverified websites as unreliable. Such information may be used for business purposes only after its authenticity and correctness have been verified.

The user is responsible for all possible consequences arising from unauthorized or inappropriate use of Internet services or content.

3.9 E-mail and other message exchange methods

In accordance with *ISMS-027 Policy, Information Transfer* as well as *ISMS-028 Policy, Information Classification*, the Information Security Manager determines the communication channel that may be used for each type of data, as well as possible restrictions on who is allowed to use communication channels, i.e. defines which activities are forbidden.

If users receive spam email messages, they must notify, via the defined procedure, the Information Security support team. Users must utilize extreme caution when opening email attachments received from unknown senders that may contain viruses, malware, email bombs, or a Trojan horse code.

If sending a message with a confidentiality label, the user must protect it as specified in the *ISMS-028 Policy, Information Classification*

Each e-mail message must contain a disclaimer, except messages sent through communication systems determined by Information Security Manager. Postings by Users from a Stefanini email address to

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 293

newsgroups or social media sites must contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Stefanini, unless posting is in the course of business duties.

3.9.1 Prohibited Email and Communications Activities

- Sending unsolicited email messages from Stefanini owned email systems, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Accessing other Users' email without their consent.
- Any form of harassment via email, telephone, or paging, whether through language, frequency, or size of messages.
- Unauthorized use or forging of email header information.
- Solicitation of email for any other email address other than that of the User's account with the intent to harass or to collect replies.
- Creating or forwarding "chain letters," "Ponzi," or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within Stefanini's networks on behalf of, or to advertise, any service hosted by Stefanini or connected through Stefanini's network.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam) or Internet blogs.

3.9.2 Blogging / Social Networking

- Blogging by users, whether using Stefanini's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Use of Stefanini's systems to engage in blogging is a local site decision. Where allowed, limited and occasional use of Stefanini's systems to engage in blogging is acceptable provided that it is done in a professional and responsible manner, does not otherwise violate Stefanini's policy, is not detrimental to Stefanini's best interests, and does not interfere with an employee's regular work duties. Blogging from Stefanini's systems is also subject to monitoring.
- *ISMS-028 Policy, Information Classification* also applies to blogging. As such, users are prohibited from revealing any Stefanini confidential or proprietary information, restricted information, trade secrets or any other material covered by Stefanini's Information Classification Policy when engaged in blogging.
- Users shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of Stefanini and/or any of its employees. Users are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by Stefanini's Non-Discrimination and Anti-Harassment policies.
- Users may also not attribute personal statements, opinions or beliefs to Stefanini when engaged in blogging. If a user is expressing his or her beliefs and/or opinions in blogs, the user may not, expressly or implicitly, represent themselves as an employee or representative of Stefanini. Users assume any and all risk associated with blogging.
- Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, Stefanini's trademarks, logos and any other Stefanini intellectual property may also not be used in connection with any blogging activity unless prior authorization has been given.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 294

3.10 Copyright

Users must not make unauthorized copies of software owned by the organization, except in cases permitted by law, by the owner or Information Security Manager. The following activities are prohibited:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Stefanini.
- Unauthorized copying of copyrighted material, including, but not limited to, the digitization and distribution of photographs from magazines, books, or other sources; music; and the installation of any copyrighted software for which Stefanini or the end user does not have an active license.
- Exporting software, technical information, encryption software, or technology, in violation of international or regional export control laws, is illegal. The Information Security Manager must be consulted prior to export of any material that is in question.

3.11 Mobile computing

Please refer to *ISMS-047, Policy, Mobile Device and Teleworking.*

Note: For Stefanini Colombia, the instruction to use in the Teleworking process is IN-RH-37 Política Teletrabajo.

3.12 Monitoring the use of information and communication systems

Although Stefanini's network administration desires to provide a reasonable level of privacy, Users should be aware that all data which is created, stored, sent or received through the information system or other organization's communication systems, including various applications, e-mail, Internet, fax, etc., whether it is personal or not, is considered the ownership of Stefanini.

For Information Assurance and Network Monitoring purposes, authorized individuals within Stefanini may monitor equipment, systems, and network traffic at any time, Users agree that authorized persons from the organization may access all such data.

Stefanini reserves the right to audit networks and systems on an as needed basis to ensure compliance with this policy and provide the highest level of security for its infrastructure. The organization may use specialized tools for the purpose of identifying and blocking forbidden methods of communication and filtering forbidden content.

All Stefanini Employees will be made aware of their rights to privacy as outlined in Stefanini's privacy policies.

3.13 Incidents

Each employee, supplier or third person who is in contact with data and/or systems of Stefanini must report any system weakness, incident or event pointing to a possible incident as specified in the *ISMS-023 Procedure, Incident management* .

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 295

4. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
Authorizations for software installation, use of Java applications and Active X controls, use of cryptographic tools, download of program code from external media, installing peripheral devices – email	Service Desk ticketing system	Backup System	Backup System	Backup System
Authorization for teleworking	Service Desk Ticketing System	Backup System	Backup System	Backup System

5. Document management

The owner of this document is the Information Security Manager, who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria must be considered:

- number of incidents related to unacceptable or unauthorized use of information assets
- number of incidents related to inappropriate employee training or awareness programs regarding acceptable use of information assets

A current version of this document is available to all staff and under version control on the corporate document control system.

6. Appendices

- Not applicable

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 296

7. Change history

Date	Version	Created by	Description of change
22-JAN-2014	1.0	Rodrigo Ricci	Document creation
11-AUG-2015	2.0	Matthew Engler	Clarified assets being taken off-site and the responsibility for return
31-OUT-2016	3.0	Larissa Longo	Added reference to ISMS-069 (Off-boarding procedure)
24-AUG-2020	4.0	Licsileth Palma	Added reference to instructions: IN-SI-01 Instructivo de Off-Boarding and IN-RH-37 Política Teletrabajo

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 297

stefanini
POWERING YOUR BUSINESS

CHANGE MANAGEMENT POLICY

Information Security Management System



Code:	ISMS-011
Version:	2.0
Date of version:	24-AUG-2020
Created by:	Licsileth Palma
Approved by:	Washington Souza
Confidentiality level:	Internal Use

Table of contents

1. PURPOSE, SCOPE AND USERS 3
2. REFERENCE DOCUMENTS 3
3. DESCRIPTION 3
4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 3
5. DOCUMENT MANAGEMENT 3
6. APPENDICES 4
7. CHANGE HISTORY 4

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 299

1. Purpose, scope and users

The purpose of this document is to define how changes to information systems are controlled.

This procedure applies to Stefanini Employees, sub-contractors, consultants, business associates, and other workers at Stefanini, including all personnel affiliated with third parties and subsidiaries on the Stefanini infrastructure (collectively “User(s)”).

2. Reference documents

Documents associated or linked are listed below:

- ISO/IEC 27001 standard, 8.1, A.12.1.2, A.14.2.2, A.14.2.3, A-14.2.4.
- ISMS-001 Policy, Information Security

3. Description

Each change to operational or production systems must be made in the following way:

1. Change may be proposed by systems’ users or managers.
2. Change must be authorized by the designated Change Committee, who must assess its justification for business and potential negative security impacts.
3. Change must be implemented by the system’s support or development team.
4. Tester is responsible for checking that the change has been implemented in accordance with the requirements.
5. Tester is responsible for testing and verifying the system's stability – the system must not be put into production before thorough testing has been conducted, if a development environment is available.
6. Implementation of changes must be reported to all persons related to the request and those that may be impacted.

Change management records are created and maintained as described in the specific change procedures.

Note: For Stefanini Colombia, the procedure to use is **Gestión del Cambio TI PC-SI-02.**

4. Managing records kept on the basis of this document

- Not applicable

5. Document management

The owner of this document is the Change Manager, who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria must be considered:

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 300

- number of incidents related to bad function of new releases of applications
- number of incidents related to inadequate changings

A current version of this document is available to all staff and under version control on the corporate document control system.

6. Appendices

- Not applicable

7. Change history

Date	Version	Created by	Description of change
22-JAN-2014	1.0	Rodrigo Ricci	Document creation
24-AUG-2020	2.0	Licsileth Palma	The use of the PC-SI-02 procedure is included for Colombia.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 301

CHECKING OF LOG OF ACCESS AND USE OF SYSTEMS PROCEDURE

Information Security Management System



Code:	ISMS-012
Version:	3.0
Date of version:	27-AUG-2020
Created by:	Licsileth Palma
Approved by:	Washington Souza
Confidentiality level:	Internal Use

Table of contents

1. PURPOSE, SCOPE AND USERS 3

2. REFERENCE DOCUMENTS 3

3. DESCRIPTION 3

3.1 RESPONSIBILITY 3

3.2 CHECKING OF LOGS 3

4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 4

5. DOCUMENT MANAGEMENT 4

6. APPENDICES 5

7. CHANGE HISTORY 5

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 303

1. Purpose, scope and users

Set tasks for the purpose of reviewing the audit records generated and detect any deviation or security incident information.

Monitoring and control systems allow you to check the effectiveness of the implemented controls.

Users of this document are the Information Security Manager and the Information Security Management team.

2. Reference documents

Documents associated or linked are listed below:

- ISO/IEC 27001 standard, 9.1, A.12.4.1, A.12.4.3.
- ISMS-001 Policy, Information Security

3. Description

3.1 Responsibility

The Information Security Manager, in cooperation with the Infrastructure and Support team, is responsible for ensuring that audit logs are generated by systems and applications, that the protection of such logs is made and that all incidents detected as a result of log data are reported.

3.2 Checking of logs

Audit logs should be maintained of all potentially important security information, enabling further research and monitoring of access and events related to sensitive operations.

The audit logs should include sufficient information to clearly identify the user or computer (by IP address) involved, the date and time, and a detail of the action recorded.

The sensitive events audit log should be always on.

Some of these are:

- Unauthorized access to systems, files and programs.
- Events associated with access control systems.
- Antivirus systems.
- Errors systems.

Access to audit logs is controlled by the System or Application Manager and any right of access must be properly authorized, documented and justified.

The review of audit logs is critical for purposes of timely detection of any unauthorized activity that may be kept by users or third parties, and to prevent the successful completion of attacks on systems and applications.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 304

Under this the Information Security Manager should carry out a weekly monitoring of the logs generated by the various systems and applications, especially those that can provide evidence of attacks or unauthorized activity. Examples of these are: Firewall, Email, Network Access, and Access for critical applications.

In order to review the logs generated must respect and follow the following steps:

- The Information Security Manager, in cooperation with the Infrastructure and Support team, will designate a location for logs to be stored.
- The Information Security Manager or the Information Security Management team must access logs and audit systems as required, depending upon the received alarms (via email or other source), from the affected applications. This will help to determine the relevance of the received alarm and whether a more thorough investigation is required.
- The Information Security Manager or the Information Security Management team must verify that the feature set for automatic synchronization of clocks is working properly.
- The Information Security Manager or the Information Security Management team, based on predetermined criteria, identify those records that may be indicating unauthorized actions, attacks, etc. and record the incident in the computer system.
- The Information Security Manager or the Information Security Management team, where it considers a situation or event to be critical, must proceed immediately to take corrective measures and follow the Incident Response plan.

4. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
Logs of access and use of systems	Systems and Applications servers	Infrastructure and Support Department	Backup procedure	US/EMEA/APAC: 7 years Brazil: 2 years or according to legal requirement Colombia:5 years or according to legal requirement

5. Document management

The owner of this document is the Information Security Manager, who must check and, if necessary, update the document at least once a year.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 305

When evaluating the effectiveness and adequacy of this document, the following criteria must be considered:

- number of incidents detected
- completeness and correctness of logs

A current version of this document is available to all staff and under version control on the corporate document control system.

6. Appendices

- Not applicable

7. Change history

Date	Version	Created by	Description of change
22-JAN-2014	1.0	Matthew Engler	Document creation
11-AUG-2015	2.0	Matthew Engler	Combined NH and SH documents into one, including the responsibilities of the Infrastructure teams.
27-AGO-2020	3.0	Licsileth Palma	Records management is added for Colombia - 5 years

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 306

TRAINING AND AWARENESS PROCEDURE

Information Security Management System



Code:	ISMS-013
Version:	4.0
Date of version:	28-AUG-2020
Created by:	Matthew Engler
Approved by:	Washington Souza
Confidentiality level:	Internal Use

Table of contents

1. PURPOSE, SCOPE AND USERS 3
2. REFERENCE DOCUMENTS 3
3. DESCRIPTION 3
3.1 TRAINING AND AWARENESS 3
3.1.1 COMPETENCE 3
3.1.2 NEEDS IDENTIFICATION 3
3.1.3 TRAINING AND AWARENESS PLAN 3
3.2 EFFECTIVENESS 4
4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 4
5. DOCUMENT MANAGEMENT 4
6. APPENDICES 5
7. CHANGE HISTORY 5

1. Purpose, scope and users

The purpose of this procedure is to describe how to identify training and awareness needs, planning, control and record these actions.

This procedure applies to Stefanini Employees, sub-contractors, consultants, business associates, and other workers at Stefanini, including all personnel affiliated with third parties and subsidiaries on the Stefanini infrastructure (collectively “User(s)”).

2. Reference documents

Documents associated or linked tare listed below:

- ISO/IEC 27001 standard, 5.2, 7.4, A.7.2.2.
- ISMS-001 Policy, Information Security

3. Description

3.1 Training and awareness

3.1.1 Competence

The organization shall ensure that all personnel who have assigned responsibilities defined in the ISMS are competent to perform the required tasks:

- Determining the necessary competence for personnel performing work affecting the ISMS skills;
- Providing training or performing other actions (eg, hiring competent personnel) to meet those needs;
- Checking the effectiveness of the actions taken, and
- Maintaining records of education, training, skills, experience and qualifications

The verification of competence is performed during the new hire recruiting process or when a change in role or function occurs. HR, Recruiting or the department manager is responsible for assessing such competence.

3.1.2 Needs identification

Top Management Representatives can identify lack of training or awareness from audits results, performance on achieving objectives or changes that can affect the ISMS.

The Information Security Manager can identify lack of training or awareness from the incidents, changes and results of the operational controls.

Any manager can identify lack of training or awareness from results of the operational control, objectives measurements, new technologies, new systems, and changes.

Frequent awareness on ISMS policies has to be provided.

3.1.3 Training and awareness Plan

Minimum required training will be defined for each job role within the ISMS and documented within a Training Plan Matrix or training agenda. At a minimum, training will be conducted upon hire and annually there after.

Any gaps in training are identified by the supervisor and action/training plans defined and maintained by the HR area or supervisor.

3.2 Effectiveness

Training and awareness actions have to have its effectiveness verified by a defined method. This may include Service Level Performance, End User Survey results, Call/Ticket Monitoring, Quality defects due to lack of training.

The method and result of the effectiveness verification is recorded and controlled by the HR area or Department Manager.

Note: for Stefanini Colombia, the procedure to use is Capacitación de Personal (PC-RH-06) and Registro Gestión Capacitación y Formación **FR-RH-15**

4. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
Training records	BRASIL/URUGUAY HR cabinet or scanned documents on the system US/APAC/EMEA employees are stored in PeopleSoft US/APAC/EMEA Contractors are stored locally with the project Employees from COLOMBIA are stored at se almacenan en el repository corresponding to the training area	HR people	HR and Supervisor	BRASIL/URUGUAY HR Records are stored for a period of 2 years after the employee leave Stefanini US/APAC/EMEA: Records are stored for a period of 2 years after the employee leave Stefanini COLOMBIA: records are stored for a period of 5 years.

5. Document management

The owner of this document is the HR, who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria must be considered:

- number of incidents related to misuse of passwords by unauthorized persons
- number of incidents related to inadequate handling of passwords

A current version of this document is available to all staff and under version control on the corporate document control system.

6. Appendices

- Not applicable

7. Change history

Date	Version	Created by	Description of change
22-JAN-2014	1.0	Larissa Longo	Document creation
04-SEP-2014	2.0	Matthew Engler	Clarified documentation requirement for section 3.1.3 to include training agenda.
29-NOV-2019	3.0	Licsileth Palma	Included for Colombia use of procedure PC-RH-06-Capacitación de Personal and Registro Gestión Capacitación y Formación **FR-RH-15**
28-AUG-2020	4.0	Matthew Engler	Clarified training requirements to be upon hire and annually.

CONFIDENTIALITY AGREEMENT POLICY

Information Security Management System



Code:	ISMS-014
Version:	3.0
Date of version:	01-JUL-2020
Created by:	Elaine Pinheiro
Approved by:	Washington Souza
Confidentiality level:	Internal Use

Table of contents

1. PURPOSE, SCOPE AND USERS 3
2. REFERENCE DOCUMENTS 3
3. DESCRIPTION 3
3.1 RESPONSIBILITIES 3
3.2 CONFIDENTIALITY AGREEMENTS 3
4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 4
5. DOCUMENT MANAGEMENT 5
6. APPENDICES 5
7. CHANGE HISTORY 5

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 313

1. Purpose, scope and users

This policy is created to define and establish the requirements for confidentiality agreements and non-disclosure signed between Stefanini and its employees, suppliers and third parties in general, so as to ensure the protection of information requirements by the company.

This policy applies to Stefanini Employees, sub-contractors, consultants, business associates, and other workers at Stefanini, including all personnel affiliated with third parties and subsidiaries on the Stefanini infrastructure (collectively “User(s)”).

2. Reference documents

Documents associated or linked are listed below:

- ISO/IEC 27001 standard, 4.2; A 7.1.2, A 7.2.1, A 15.1.3, A.18.1.1.
- ISMS-001 Policy, Information Security
- Confidentiality Statement
- Suppliers Confidentiality Agreement

3. Description

3.1 Responsibilities

- Managers / asset owners must ensure that any new relationship with staff, suppliers, or third parties, sign a confidentiality agreement with Stefanini.
- Information Security Manager must evaluate, together with the support of legal counsel and HR, annually, the need to make changes or additions to the format established for confidentiality agreements, so as to ensure their effectiveness and compliance with legal and regulatory aspects.

3.2 Confidentiality Agreements

Stefanini must maintain signed confidentiality statements with all its employees, providers and third parties that may require access to information assets of the company. This signature may be on paper form or electronic.

Managers / owners of the assets should ensure that any new relationship with staff, suppliers, or third parties, sign a confidentiality agreement with Stefanini. Agreements will be signed by the appropriate parties and access controlled per appropriate Data Handling standards.

3.2.1 Format of the Agreements.

Confidentiality agreements should consider at least the following:

- A definition of the information to be protected.
- Expected duration of the agreement.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 314

- Actions required to finalize the deal.
- Responsibilities of the signatories.
- Ownership of Information.
- The permitted use of the information.
- The right to audit and monitor activities.
- Report incidents, violations.
- Return or destruction of information.
- Other items that may be required by the departments and / or legal or regulatory reasons.

3.2.2 Review of Agreements.

The statements will be reviewed annually by the Information Security Manager with the assistance of legal counsel and HR, in order to identify and incorporate any aspect necessary for the purpose of ensuring its effectiveness and relevance to the legal and regulatory issues that may have arisen. This review may be informal if no changes are to be made, depending upon the legal requirements of a country.

Evidence of this review shall be documented by the response given by the Legal Adviser.

4. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Control for record protection	Retention time
Confidentiality Statement	HR cabinet	Human Resource Analyst	Only Top Management Representative, Information Security Manager or HR / Payroll staff is authorized to access data.	Brazil/Uruguay: At least 5 years after no longer performing work for the company US/EMEA/APAC:/Colombia Per the Records Retention Policy
Suppliers Confidentiality Agreement	Administrative cabinet; Shared Drive	Administrative Department; Legal	Only Top Management Representative, Information Security Manager, Legal Counsel is authorized to access data.	At least 2 years after no longer performing work for the company
Response from Legal Adviser	Information Security Manager cabinet; Shared	Information Security Manager; Legal.	Only Top Management Representative, Information Security	At least 2 last review

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 315

	Drive		Manager, Legal Counsel is authorized to access data	

5. Document management

The owner of this document is the Information Security Manager, who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria must be considered:

- Legal requirements
- Audits results

A current version of this document is available to all staff and under version control on the corporate document control system.

6. Appendices

- Not applicable

7. Change history

Date	Version	Created by	Description of change
22-JAN-2014	1.0	Larissa Longo	Document creation
11-AUG-2015	2.0	Matthew Engler	Updated to allow for electronic signature; Informal review is allowed to address some country-specific legalities.
01-JUL-2020	3.0	Elaine Pinheiro	Reviewed due the news sites in scope

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 316

RECRUITMENT PROCEDURE

Information Security Management System



Code:	ISMS-015
Version:	3.0
Date of version:	27-AUG-2020
Created by:	Licsileth Palma
Approved by:	Washington Souza
Confidentiality level:	Internal Use

Table of contents

1. PURPOSE, SCOPE AND USERS 3

2. REFERENCE DOCUMENTS 3

3. DESCRIPTION 3

3.1 RECRUITMENT 3

3.1.1 JOB DESCRIPTION 3

3.1.1. Information on candidate experience 3

3.1.2. Personal and financial background checks 3

3.2 APPROVAL 3

4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 4

5. DOCUMENT MANAGEMENT 4

6. APPENDICES 4

7. CHANGE HISTORY 4

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 318

1. Purpose, scope and users

The purpose of this procedure describes the minimum recruitment tasks and criteria to be used when hiring new employees.

This procedure applies to all employees that can affect the Information Security Management System (ISMS).

Users of this document are HR / Recruiting departments of Stefanini.

2. Reference documents

Documents associated or linked tare listed below:

- ISO/IEC 27001 standard, 7.2, A 7.1.1.
- ISMS-001 Policy, Information Security

3. Description

3.1 Recruitment

3.1.1 Job Description

The candidates are evaluated in accordance with the Job Description requirements on experience, skills and education. The job description can be used to define the competencies as well.

3.1.1. Information on candidate experience

After being pre-approved on Job Description requirements, the HR / Recruiting department collects all information from the candidate related to his/her professional experience, by interview, resume / CV or other documentation.

The HR / Recruiting department checks all the information with the candidate and with his/her previous employer, as far as possible. When it is not possible to perform this check, the HR / Recruiting department will document as such during the interview process.

3.1.2. Personal and financial background checks

In accordance with local law, the HR / Recruiting department performs a background check on the candidate. This check should include historical information regarding personal, criminal and financial behavior.

Note: In Stefanini Colombia, the procedure to be used is **Talent Acquisition (PC-RH-05).**

3.2 Approval

The HR / Recruiting department and the Manager who is hiring approve the candidate making sure that he/she complies with all requirements.

The employee attends to induction training.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 319

4. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
Records of competence	HR cabinet or scanned documents on the system	HR / Recruiting Personnel	Only HR / Recruiting personnel can access the files.	Records are stored for a period of 2 years after the employee leave Stefanini

5. Document management

The owner of this document is the Recruiting Manager or equivalent, who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria must be considered:

- Standard changes

A current version of this document is available to all staff and under version control on the corporate document control system.

6. Appendices

- Not applicable

7. Change history

Date	Version	Created by	Description of change
22-JAN-2014	1.0	Larissa Longo	Document creation
12-MAI-2014	2.0	Cleverton Oliveira	Included the job description to be used to define the competences.
27-AUG-2020	3.0	Licsileth Palma	Included for Colombia the Talent Acquisition Process (PC-RH-05)

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 320

ON-BOARDING OF PERSONNEL PROCEDURE

Information Security Management System



Code:	ISMS-016
Version:	2.0
Date of version:	27-AUG-2020
Created by:	Licsileth Palma
Approved by:	Washington Souza
Confidentiality level:	Internal Use

Table of contents

1. PURPOSE, SCOPE AND USERS 3

2. REFERENCE DOCUMENTS 3

3. DESCRIPTION 3

3.1. PREPARATION FOR ON-BOARDING 3

3.2. IMMEDIATE ACTIONS 4

3.3. SUBSEQUENT ACTIONS 5

4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 5

5. DOCUMENT MANAGEMENT 5

6. APPENDICES 5

7. CHANGE HISTORY 6

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 322

1. Purpose, scope and users

The purpose of this document is to describe the mechanism and criteria used in Stefanini for the integration of new staff to the company.

This policy applies to Stefanini Employees, sub-contractors, consultants, business associates, and other workers at Stefanini, including all personnel affiliated with third parties and subsidiaries on the Stefanini infrastructure (collectively "User(s)").

2. Reference documents

Documents associated or linked are listed below:

- ISO/IEC 27001 standard, 5.1, 7.3, 7.4, A.7.1.2, A.7.2.1
- ISMS-001 Policy, Information Security
- ISMS-013 Procedure, Training and Awareness
- Confidentiality Statement

3. Description

Every person who joins the company receives basic general information on the Information Security Management System (ISMS).

On-boarding objectives are:

- Setup of the new hire's work environment in a timely manner.
- Provide proper training of the new hire to prepare them for the various work tasks they will be assigned.
- Understand the fundamental principles of the company, its organization, its Mission, Vision, Quality Policy and Information Security Policy.
- Establish the first connections with the company and ensure the new hire is integrated into the existing team.
- Ensure new hire is adapting to their team members and has a positive image of the company.

Note: In Stefanini Colombia, the procedure to use is the **Organizational Onboarding PC-RH-15** and the **Onboarding Instructions IN-RH-42**

3.1. Preparation for On-Boarding

Activity	Responsible
Once the start date of the new hire has been confirmed, HR will: ▪ Confirm the start date to the relevant Manager to ensure a plan is in	HR and New Hire's Manager

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 323

Activity	Responsible
place for the new hire in their first week. ▪ Process the new hire so that account credentials to the system along with a work area can be setup. This may follow a defined technology on-boarding process. ▪ Ensure training in Security and Quality principles	

If the New Hire's Manager decides to provide specific training, they should follow the mechanisms described in the Training and awareness Procedure.

3.2. Immediate Actions

Activity	Responsible
Beginning on their first day, the new hire is presented with the materials relevant to their job, which may include: ▪ Handbook ▪ Job Description ▪ Organization ▪ Employment contract ▪ Other informational materials ▪ Information Security Policy ▪ Confidentiality Statement (which includes agreement with the ISMS)	HR
The new hire is introduced to all relevant staff and taught about the physical facilities of the company.	HR or New Hire's Manager
The employee manager or his designated representative explains in detail the information contained in the Job Description.	New Hire's Manager
Should consider awarding a supervisor / manager to accompany the first period of integration in the area and is a benchmark for consultation, support and information.	New Hire's Manager
Deliver basic stationery materials.	HR or New Hire's Manager
Ensure the new hire is placed in the necessary applications, including the employee / contractor database.	HR or New Hire's Manager

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 324

3.3. Subsequent Actions

Activity	Responsible
The new employee must provide to Human Resource: ▪ Signed Contract (if applicable) ▪ Signed Confidentiality Statement ▪ Copy of academic degree, certificates of study and school (if required) ▪ Health Library (if applicable)	HR

4. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Control for record protection	Retention time
Confidentiality Statement	HR cabinet or scanned documents on the system	Human Resources	Only HR staff or other personnel with a "need to know" are authorized to access data.	Brazil: Records are stored for a period of 5 years after the employee leave Stefanini US/EMEA/APAC: Per Record's Retention Policy

5. Document management

The owner of this document is the HR department, who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria must be considered:

- Induction records
- Reports and audit results

A current version of this document is available to all staff and under version control on the corporate document control system.

6. Appendices

- Not applicable

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 325

7. Change history

Date	Version	Created by	Description of change
22-JAN-2014	1.0	Larissa Longo	Document creation
27-AUG-2020	2.0	Licsileth Palma	Included for Colombia, the procedure to be used is the Organizational Onboarding (PC-RH-15) and the Onboarding Instructions IN-RH-42

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 326

DISCIPLINARY PROCEDURE

Information Security Management System



Code:	ISMS-017
Version:	2.0
Date of version:	24-AUG-2020
Created by:	Licsileth Palma
Approved by:	Washington Souza
Confidentiality level:	Internal Use

Table of contents

1. PURPOSE, SCOPE AND USERS 3
2. REFERENCE DOCUMENTS 3
3. DESCRIPTION 3
3.1. DISCIPLINARY PROCEDURE 3
4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 4
5. DOCUMENT MANAGEMENT 4
6. APPENDICES 4
7. CHANGE HISTORY 4

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 328

1. Purpose, scope and users

The purpose of this document is to define the disciplinary actions and rules for violations of the policies, statement, agreement and acceptable use of the ISMS.

This policy applies to Stefanini Employees, sub-contractors, consultants, business associates, and other workers at Stefanini, including all personnel affiliated with third parties and subsidiaries on the Stefanini infrastructure (collectively “User(s)”).

2. Reference documents

Documents associated or linked are listed below:

- ISO/IEC 27001 standard, 7.3.2, A.7.2.3
- ISMS-001 Policy, Information Security
- ISMS-013 Procedure, Training and Awareness
- Confidentiality Statement

3. Description

3.1. Disciplinary procedure

ISMS has established acceptable use and practices for Information Security. These policies and practices are communicated to all users.

The legal and regulatory requirements count on the analysis of any situation or issue.

Any violation or inappropriate use of the equipment or systems identified must be analysed and disciplinary actions must be taken or, registered for why they were not.

Human Resources, Information Security Manager and the involved department manager must investigate the situation and make an appropriate decision. This decision may seek outside help from law professionals or technical experts.

Additional deciding factors include:

- Nature of the situation
- Gravity of the violation
- Impact on information security and business continuity
- Related laws or regulatory requirements
- Recurrence of the violation (i.e. if the user has been involved in other situations)

Information related to the situation, along with deciding factors, are properly documented.

The disciplinary action is communicated to the user by his/her manager (or appropriate supervisor / contact) and, if necessary, the Information Security Manager.

Note: For Stefanini Colombia, the instruction to use is Reglamento Interno de Trabajo IN-RH-33.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 329

4. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
Report on Disciplinary Procedure	HR Personnel File	Human Resources	Only Human Resources or other designated personnel with a "need to know" may access the files.	Brazil: Records are stored for a period of 5 years after the employee leave Stefanini US/EMEA/APAC: Per the Records retention Policy

5. Document management

The owner of this document is Human Resources, who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria must be considered:

- Results of management review
- Audits results

A current version of this document is available to all staff and under version control on the corporate document control system.

6. Appendices

- Not applicable

7. Change history

Date	Version	Created by	Description of change
22-JAN-2014	1.0	Larissa Longo	Document creation
24-AUG-2020	2.0	Licsileth Palma	The use of IN-RH-33-Reglamento Interno de Trabajo is included for Colombia

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 330

stefanini
POWERING YOUR BUSINESS

ASSET IDENTIFICATION AND VALUATION PROCEDURE

Information Security Management System



Code:	ISMS-018
Version:	3.0
Date of version:	12-AGO-2015
Updated by:	Matthew Engler
Approved by:	Washington Souza
Confidentiality level:	Internal Use

Table of contents

1. PURPOSE, SCOPE AND USERS 3
1.1. RESPONSIBILITIES 3
1.2. DEFINITIONS AND ABBREVIATIONS 3
2. REFERENCE DOCUMENTS 3
3. DESCRIPTION 3
3.1. SYSTEMATIC APPROACH 3
3.2. INFORMATION ASSETS OWNERS IDENTIFICATION 4
3.3. PROCESS IDENTIFICATION 4
3.4. ASSETS IDENTIFICATION 4
3.5. COMPILATION OF INFORMATION ASSETS 6
3.6. ASSETS VALUATION 6
3.7. GROUP VALUATION 7
3.8. FOCUS, AUTHORIZATION AND PRIORITY OF ASSETS FOR THE CURRENT YEAR 7
3.9. ASSETS UPDATES 7
4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 7
5. DOCUMENT MANAGEMENT 8
6. APPENDICES 8
7. CHANGE HISTORY 8

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 332

1. Purpose, scope and users

This procedure establishes guidelines and standards for the identification of information assets as part of the establishment and maintenance of Stefanini´s Information Security Management System (ISMS). This document explains the process for identifying assets in its initial implementation as well as the subsequent activities in the PDCA (Plan, Do, Check, Act) cycle of continuous improvement.

This policy applies to Stefanini Employees, sub-contractors, consultants, business associates, and other workers at Stefanini, including all personnel affiliated with third parties and subsidiaries on the Stefanini infrastructure (collectively “User(s)”).

1.1. Responsibilities

The Information Security Manager is responsible for:

- Ensuring the update of the Assets List once a year.
- Giving value to the identified information assets, as well as the update and incorporation of new assets to the consolidated list

The managers / asset owners are responsible for:

- Informing the Information Security Manager of the incorporation of new assets to the list
- Approving the Assets List and classification during annual reviews.

1.2. Definitions and Abbreviations

Asset: Anything that holds value to the organization (ISO IEC 13335-1:2004).

Security Committee: Information Security Management System governance team.

2. Reference documents

Documents associated or linked are listed below:

- ISO/IEC 27001 standard, A 8.1
- ISMS-001 Policy, Information Security
- Risks, Assets and Classification Spreadsheet (Risks, Assets and Classification.xlsx)
- Asset Valuation_Risk Treatment_Owners {year} (xlsx)

3. Description

3.1. Systematic Approach

The identification and compilation of assets is the first step in Stefanini´s risk assessment methodology.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 333

3.2. Information Assets owners identification

With management support, the Asset Management team identifies the asset owners and compiles the list.

3.3. Process Identification

The main business processes are identified, within the capacity of the Information Security Management System.

3.4. Assets Identification

The Information Security Manager, along with the asset owners, review and evaluate the processes and identify the information and other assets relevant to the information security management system.

The Information Security Manager reviews the Assets List yearly, updating it whenever necessary. The asset owners approve the review.

Each information asset is classified and grouped so as to allow a risk assessment study of a group of similar assets.

All the data collected for each Information Asset is listed below:

- **Type**
  - Classification according to the Information Asset

Type	Description
(DI) Digital	Information elements that are grouped or individual and in some way represents knowledge to the organization. Digital Data is the main type of asset that allows the organization to provide its services. It is, in a way, an abstract asset that will be stored on computers or information systems (usually grouped as database) or will be transferred from one place to another using data transmission means. It is common that in a risk and impact analysis, the user only gives value to the data, considering the other assets nothing but servers that must protect and care for the data entrusted to them.
(ES) External Services	Services that the company has attributed to third parties in order to fulfil its requirements.
(SW) Software	With multiple names (programs, applications, development, etc.) this item refers to tasks that have been automated by computer equipment. The applications manage, analyze and transform data, allowing information to be exploited for services provision. This item does not cover the so called "Source Code", which is commercial valued data to be protected as such. Such code would look like Digital (DI) data.
(HW) Hardware	Hardware is physical, material good created to, directly or indirectly, support the services provided by the organization, being temporary or permanent data repositories, application execution supporters or responsible for the processing or transmission of data.
(PL)People	This item refers to people related to the information systems.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 334

(IM) Image and Prestige	This item refers to the company´s image and reputation
(IP) Intellectual Property	This item refers to any product of the human intellect that the law protects from unauthorized use by others. Intellectual property is traditionally comprised of four categories: patent, copyright, trademark, and trade secrets.
(PR) Print	This item includes all documentation in a printed format.
(DB) Database	This item includes all the databases physical and logical.
(DS) Disk	This item includes all kind of device that has logical information, like: CDs, DVDs, External HD, and others.
(MB) Mobile	This item includes all kind of device mobile, like cellphones, smartphones, and others.

- **Processes**
  - Main processes identified within the ISMS reach
- **Group**
  - The assets are grouped so as to allow risk evaluation of a set of similar assets.
  - Groups are formed by crossing their Type with their Process/Procedure, within the ISMS reach (Group = Type/ Process/Procedure).
- **Description**
  - Brief description of the Asset
- **Location**
  - Classification according to the asset location

Location
Stefanini Facility
User's Assigned Equipment
Outside of the Country
Server Room (Stefanini)
Datacenter (Non-Stefanini)

- **Responsible**
  - Person responsible for the asset
- **Classification**
  - Public
  - Internal Use

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 335

- Confidential
- Restricted

- **Confidentiality, Integrity and Availability values**
  - Low
  - Medium
  - High
  - Critical
- **Explanation**
  - Any kind of observation about the asset

3.5. Compilation of information assets

The compiled assets are input in the *Assets – Classification* sheet of the *Risks, Assets and Classification* Spreadsheet, or other Asset Management tool.

3.6. Assets valuation

Once compiled, the assets are analyzed by the Information Security Manager and receive values based on their importance to the business, according to the information security criteria (**Confidentiality, Integrity and Availability**).

By following this procedure, Confidentiality, Integrity and Availability values are determined for each asset.

Below is the scale of assets valuation to assess the Confidentiality, Integrity, Availability criteria (Note, for items which are Not Applicable, the value is 0):

Asset Valuation			
	Confidential	**Integrity**	**Availability**
Low = 1	Refers to open information, information processing means and resources, which is freely accessible to anyone. Example: information on the website of the company.	Refers to all information, information processing means and resources that the loss of integrity doesn't have influence on the business of the company.	All asset that is internal use of Stefanini and that faults or problems that occur on them, prevents so as slightly the daily work of the person on the company. Examples: teams contingency.
Medium = 2	Refers to all information, means and resources that are considered internal use. It's means that the asset may be accessible by members of the company without restriction, but shouldn't be accessible by anyone external.	Refers to all information, means and resources that the integrity isn't so important, but should be maintained. For this asset, the loss of integrity has a smaller influence on the business of the company.	All asset that is internal use of Stefanini and that faults or problems that occur on them, prevents so as important the daily work of the person on the company. Examples: Development server.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 336

High = 3	Refers to all information, means and resources that are considered access restricted. It's means that the asset may be only accessible by members of the company, if they have permission.	Refers to all information, means and resources that the integrity is important and must be maintained. For this asset, the loss of integrity has a notable influence on the business of company and must be avoided.	All asset that integrates the production chain of one or more services of Stefanini and that faults or problems that occur on them, has consequences in the normal provision of these for a customer.
Critical = 4	Refers to all information, means and resources that are considerable confidential. This asset should be only accessible with explicit authorization. The impact would be serious and should be avoided in all circumstances.	Refers to all information, means and resources that the integrity is very important and must be maintained in low levels for all kind of circumstances. For this asset, the loss of integrity has a negative important influence on the business.	All asset that integrates the production chain of one or more services of Stefanini and that fault or problems that occur on them, has consequences of no normal provision of these services for many customers.

3.7. Group valuation

Once the assets valuation has been completed for all information assets, they are grouped according to the criteria established on item 3.4.

For the groups formed by crossing Types and Processes, the highest value is applied for each one of the criteria (CIA = Confidentiality, Integrity, Availability) that make up the group.

3.8. Focus, authorization and priority of assets for the current year

For each PDCA cycle, in the annual Top Management review or in the partial reviews, initiated by a review petition sent by the Security Committee or Top Management, the scope of the Information Security Management System is defined, analyzing if it should be kept or extended to other areas.

The Information Security Manager reviews the assets lists and gets the managers/processes owner approval for the future approval of the Top Management.

3.9. Assets updates

As Stefanini´s environment changes, information assets will be added, removed or changed along with their established values. Updates are carried out by the assets/processes owners as they become necessary, ensuring the Information Security Manager is informed when appropriate.

4. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Control for record protection	Retention time
Risks, Asset and Classification	ISMS Portal	Information Security Manager or someone designated by him	Only Top Management Representative or someone designated by him is authorized to edit data	Minimum of 2 years

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 337

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 338

5. Document management

The owner of this document is the Information Security Manager, who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

- Changes of asset types
- Audits
- Change of assets company

A current version of this document is available to all staff and under version control on the corporate document control system.

6. Appendices

- Not applicable

7. Change history

Date	Version	Created by	Description of change
22-JAN-2014	1.0	Juliana C Bigheti	Document creation
24-SEP-2014	2.0	Matthew Engler	Added reference document for risk owners.
12-AUG-2015	3.0	Matthew Engler	Re-assigned asset valuation responsibilities to Security Manager

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 339

stefanini
POWERING YOUR BUSINESS

RISK ANALYSIS PROCEDURE

Information Security Management System



Code:	ISMS-019
Version:	4.0
Date of version:	15-MAR-2016
Created by:	Matthew Engler
Approved by:	Washington Souza
Confidentiality level:	Internal Use

Table of contents

1. PURPOSE, SCOPE AND USERS 3

1.1. RESPONSIBILITIES 3

1.2. DEFINITIONS AND ABBREVIATIONS 3

2. REFERENCE DOCUMENTS 3

3. DESCRIPTION - RISKS METHODOLOGY 4

3.1. ASSET VALUATION 4

3.2. THREAT IDENTIFICATION AND RISK ASSESSMENT 5

3.2.1. Threat Identification 5

3.2.2. Probability the Event Occurs (Likelihood) 5

3.2.3. Vulnerabilities / Definite Cause 6

3.2.4. Exposure 6

3.2.5. Impact 6

3.2.6. Calculating the Current Risk 8

3.3. ANALYSIS PERFORMED 8

3.3.1. Identified Assets 8

3.3.2. Threats Identified 8

3.3.3. Risks Owners Identified 8

3.3.4. RiskTreatment Strategy 9

3.4. RISK RESPONSE 9

3.5. RESIDUAL RISK PROJECTED 9

3.6. FORMAL ACCEPTED OF RESIDUAL RISK 9

3.7. RISK STATUS 9

3.8. CONTINGENCY PLAN 10

4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 10

5. DOCUMENT MANAGEMENT 10

6. APPENDICES 11

7. CHANGE HISTORY 11

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 341

1. Purpose, scope and users

The purpose of this document is to describe the procedure for identification of threats, vulnerabilities, likelihood of occurrence, exposure level and risks to information security and business continuity.

The users of this document are personnel responsible for the conducting of risk assessments for the organization.

1.1. Responsibilities

It is the asset owners, process owners, the Information Security Manager and Security Committee responsibility to maintain a current Risk Assessment and to identify and measure the Risk Analysis and Management elements, respecting the capacity of the Security Information Management System.

1.2. Definitions and Abbreviations

Security Committee – Committee designed to give overall direction, guidance and approval for the Information Security Management System.

Risk refers to the probability of an event and potential consequences or impact to an organization associated with that event's occurrence. Risks do not necessarily exist in isolation from other risks; as a result, a series of risk events may result in a collective set of consequences that is more impactful than the discrete set of consequences associated with risk events taking place in isolation. Risk is inherent to any activity. It is neither possible, nor advantageous, to entirely eliminate risk from an activity without ceasing that activity.

Probability or **Likelihood** is a qualitative description of probability or frequency; chance of something happening.

Impact or **Consequence** is the outcome of an event, being a loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with an event.

Risk control means taking action to first eliminate risks so far as is reasonably practical, and if that is not possible, minimizing the risks so far as is reasonably practical. Eliminating an event will also eliminate any risks associated with that event.

Risk Assessment is the process of evaluating and comparing the level of risk against predetermined acceptable levels of risk.

Risk Management is the application of a management system to risk and includes identification, analysis, treatment and monitoring.

Risk Owner is the person(s) with the accountability and authority to manage risks and is usually the person directly responsible for the strategy, activity or function that relates to the risk.

Risk Treatment is a process to modify the risk and may involve avoiding the risk; removing the risk source; changing the likelihood; changing the consequences; transferring or sharing the risk; accepting the risk by informed decision.

2. Reference documents

Documents associated or linked are listed below:

- ISO/IEC 27001 standard, 6.1.1, 6.1.2, 6.1.3

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 342

- ISMS-001 Policy, Information Security
- ISMS-018 Procedure, Asset Identification and Valuation
- Risks, Assets and Classification Spreadsheet (Risks, Assets and Classification.xlsx)
- Asset Valuation_Risk Treatment_Owners {year} (xlsx)

3. Description - Risks Methodology

Stefanini will classify assets according to their relative value, evaluate the threats to those assets, the likelihood and vulnerability such threats could occur and establish a risk value. For risks that are **Very High** or **Extreme**, Stefanini will treat the risk to reduce the risk value. Stefanini may treat additional risks as it sees fit.

3.1. Asset Valuation

The following criteria have been established to evaluate the assets.

Values of confidentiality, integrity and availability of assets

Asset Valuation			
	Confidentiality	**Integrity**	**Availability**
Low	Refers to open information, information processing means and resources, which is freely accessible to anyone. Example: information on the website of the company.	Refers to all information, information processing means and resources that the loss of integrity doesn't have influence on the business of the company.	All asset that is internal use of Stefanini and that faults or problems that occur on them, prevents so as slightly the daily work of the person on the company. Examples: teams contingency.
Medium	Refers to all information, means and resources that are considered internal use. It's means that the asset may be accessible by members of the company without restriction, but shouldn't be accessible by anyone external.	Refers to all information, means and resources that the integrity isn't so important, but should be maintained. For this asset, the loss of integrity has a smaller influence on the business of the company.	All asset that is internal use of Stefanini and that faults or problems that occur on them, prevents so as important the daily work of the person on the company. Examples: Development server.
High	Refers to all information, means and resources that are considered access restricted. It's means that the asset may be only accessible by members of the company, if they have permission.	Refers to all information, means and resources that the integrity is important and must be maintained. For this asset, the loss of integrity has a notable influence on the business of company and must be avoided.	All asset that integrates the production chain of one or more services of Stefanini and that faults or problems that occur on them, has consequences in the normal provision of these for a customer.
Critical	Refers to all information, means and resources that are considerable confidential. This asset should be only accessible with explicit authorization. The impact would be serious and should be avoided in all circumstances.	Refers to all information, means and resources that the integrity is very important and must be maintained in low levels for all kind of circumstances. For this asset, the loss of integrity has a negative important influence on the business.	All asset that integrates the production chain of one or more services of Stefanini and that fault or problems that occur on them, has consequences of no normal provision of these services for many customers.

The assets are valued on an individual basis and then grouped by similar areas for analysis. It is this grouping for which associated risks will be evaluated. The group's value is defined as the maximum of the values of its members, for each one of the three criteria.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 343

3.2. Threat Identification and Risk Assessment

3.2.1. Threat Identification

For each category / group of identified assets, all the possible threats are determined and placed in the *Risks, Assets and Classification Spreadsheet*.

This should include the identification of organizational, legal, and other requirements, as well as situations that should be taken into account given the important goals defined by the organization.

The threat / risk written in terms of the event ("*uncertain event*") that could occur and the impact ("*effect on objective(s)*") that this would have.

The threat will also have a linked threat source. The same threat may have multiple threat sources which need to be evaluated.

3.2.2. Probability the Event Occurs (Likelihood)

Risk is characterised and rated by considering two characteristics:

1. Probability (P) or likelihood of occurrence; and
2. Impact (I) or consequence of occurrence.

This is expressed as R (risk) = P (Probability) x I (Impact).

Once the threats have been identified, the probability that the event occurs is selected. Probability is defined below:

Almost Certain	Threat is realized / event is **almost certain** to occur; or occurs **more than 100 times a year.**
Likely	Threat is realized / event is **highly likely** to occur; or occurs between **10-100 times a year.**
Possible	Threat is realized / event is **somewhat likely** to occur; or occurs between **1-10 times a year.**
Unlikely	Threat is realized / event is **unlikely** to occur; or occurs **less than once a year, but more than once every 10 years.**
Rare	Threat is realized / event is **highly unlikely** to occur; or occurs **less than once every 10 years.**

Frequency is used as a reference and the description is verified to be adequate for the organization and the assets. Only one scale is used for the entire organization and assets, so as to make results comparable.

Suggested criteria to assess the threats occurring probability
It is important to consider the historical data related to the incidents
It is important to disregard the existing controls.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 344

It is important to consider how desirable the asset is and if there is a possible interested one, inside or outside, motivated to attack, steal or modify it, and what skills are necessary to attack it.

3.2.3. Vulnerabilities / Definite Cause

Vulnerabilities / Causes are definite events or sets of circumstances which exist in the project or its environment, and which give rise to uncertainty.

The existing controls and potential vulnerabilities for each threat are identified in the *Risks, Assets and Classification Spreadsheet*. The following scale is used to give value to the probability the vulnerability is realized:

Almost Certain	If the threat event is initiated or occurs, it is **almost certain** to have adverse impacts.
Likely	If the threat event is initiated or occurs, it is **highly likely** to have adverse impacts.
Possible	If the threat event is initiated or occurs, it is **somewhat likely** to have adverse impacts.
Unlikely	If the threat event is initiated or occurs, it is **unlikely** to have adverse impacts.
Rare	If the threat event is initiated or occurs, it is **highly unlikely** to have adverse impacts.

Only one valuation is done for the set of controls associated to the same threat.

The controls list defined in ISO 27002:2013 is taken into account when judging the weakness or strength of controls.

Furthermore, it is necessary to accept that an asset may have intrinsic vulnerabilities regardless of any control. For example: it is easier to steal a notebook than it is to steal a server, just as it is easier to modify a handwritten document than to modify a printed one.

3.2.4. Exposure

According to the values of likelihood and vulnerability, we'll obtain the exposure value of the threat to the asset group. The value is obtained according to the following matrix:

Vulnerability/ Likelihood	Almost Certain	Likely	Possible	Unlikely	Rare
Almost Certain	Almost Certain	Likely	Likely	Possible	Possible
Likely	Likely	Likely	Possible	Possible	Unlikely
Possible	Likely	Possible	Possible	Possible	Unlikely
Unlikely	Possible	Possible	Possible	Unlikely	Rare
Rare	Possible	Unlikely	Unlikely	Rare	Rare

3.2.5. Impact

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 345

Impact is defined as the negative effect that, along with the assessed value of the asset, may result in the effective threat occurrence.

The following possibilities are considered in relation to impact:

- information / knowledge is lost;
- third parties could have access to Information / knowledge;
- the information has been manipulated or is incomplete;
- the information / knowledge or person is not available;
- the legitimacy of the information source is questionable.

To give value to the information elements, the following scale in taken into account:

Impact	Description
Catastrophic	The threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations.
Major	The threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations. A severe or catastrophic adverse effect means that, for example, the threat event might: (i) cause a severe degradation in or loss of project capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.
Moderate	The threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals other organizations. A serious adverse effect means that, for example, the threat event might: (i) cause a significant degradation in project capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.
Minor	The threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals other organizations. A limited adverse effect means that, for example, the threat event might: (i) cause a degradation in project capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
Insignificant	The threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals, other organizations.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 346

The value of Impact is based upon the Confidentiality, Integrity and Availability classifications of the grouped assets. Additional criteria may also be considered.

3.2.6. Calculating the Current Risk

Once asset values are defined, the impact of threats to these assets and the degree of exposure from identified threats, the current risk value is obtained:

		Probability				
		Rare	Unlikely	Possible	Likely	Almost Certain
Impact	Catastrophic	Tolerable	High	Very High	Very High	Extreme
	Major	Low	Tolerable	High	Very High	Very High
	Moderate	Low	Low	Tolerable	High	High
	Minor	Very Low	Low	Tolerable	Tolerable	High
	Insignificant	Very Low	Very Low	Low	Tolerable	Tolerable

The description of each level can be understood such as methodology used:

Level Description	
Very Low	It has a very low impact on the business operations. Doesn't require action.
Low	Minor business effects. Doesn't require action.
Tolerable	Some negative business impacts would take place. Such risks are considered acceptable. Actions could be taken but they are not considered necessary.
High	It has negative effects on the business operations. It must be considered for treatment to reduce probability.
Very High	Serious negative business impacts would take place. These risks must be reduced or handled in such a way that will turn them into acceptable.
Catastrophic	Disastrous negative business impacts would take place and such risks should be reduced under all circumstances. It is important to reduce or handle these risks differently to ensure that they won´t come to pass.

3.3. Analysis Performed

3.3.1. Identified Assets

Assets are identified, according to *ISMS-018, Asset Identification and Valuation Procedure* and detailed in the appropriate form.

3.3.2. Threats Identified

Threats are identified using generally accepted sources of threat information. Threats are documented on the *Risks, Assets and Classification Spreadsheet* under *Threats Identified* tab.

3.3.3. Risks Owners Identified

A risk owner is identified for each risk. The risk owner has the authority to manage a particular risk and is accountable for doing so.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 347

3.3.4. RiskTreatment Strategy

Risks may be managed by using one or more of the following methods:

- Eliminate (eliminate, withdraw from or do not become involved in an activity creating risk);
- Accept (accept the risk and plan for the expected impact);
- Transfer/Share (move the risk to another party by hedging against undesired outcome or reduce the risk through processes such as insurance); and,
- Mitigate (control the risk through additional or optimized controls).

Risks that are **Very High** or **Extreme** may not be Accepted without Executive Leadership approval and should be treated with one of the other methodologies.

These risks will be treated in accordance with *ISMS-020, Procedure, Risk Treatment Plan*.

These risks must be communicated to the **Security Committee**.

3.4. Risk Response

Based on existing treatment options, Stefanini will try to mitigate all the risks that are **Very High** or **Extreme**. The detail of treatment actions for each risk identified and "not acceptable", as well as control selected, can be found on the *Risks, Assets and Classification Spreadsheet* under the *Risk Treatment Plan* tab.

These controls help reduce the vulnerabilities associates with assets, and can be exploited by threats identified, reducing the final risk. However, treatments can also help to reduce the likelihood of occurrence and/or the impact to the business reducing the risk score.

3.5. Residual Risk Projected

For the risks, which are to be handled, a new residual risk value is calculated, taking the implemented controls into account. Refer to *ISMS-020, Procedure, Risk Treatment Plan*.

3.6. Formal accepted of Residual Risk

The risk owners provide formal acceptance of the risks analysis and the residual risks projected.

3.7. Risk Status

For each risk, the current status is listed:

- Identified – A risk has been identified, but no steps have been taken yet to Eliminate, Accept, Transfer / Share or Mitigate the risk.
- In Progress – A risk has been identified and some steps have been taken to either Eliminate, Transfer / Share or Mitigate the risk.
- Mitigated – A risk has been identified and all steps to Transfer / Share or Mitigate the risk have been completed.
- Accepted – A risk has been identified and the risk owner has formally acknowledged acceptance of the risk.
- Occurred – A risk has been realized.
- Retired – A risk is no longer valid because either:
    - The risk has been eliminated through an action.
    - The actual probability / exposure has been reduced to Rare. Note: A risk may remain in the register even if actual probability / exposure is Rare at the request of the Risk Owner.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 348

3.8. Contingency Plan

If applicable, a contingency plan can be listed. This plan should document what could be done to minize the impact if a risk were realized. Costs for this plan can be calculated and validated if necessary.

4. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Control for record protection	Retention time
Risks, Assets and Classification	ISMS Portal	Information Security Manager or someone designated by him	Information Security Manager or someone designated by him is authorized to edit data	2 years

5. Document management

The owner of this document is the Information Security Manager, who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

- Number of assets
- Number of threats
- Number of threats by asset
- Number of risks by asset
- Number of initiated corrective actions
- Number of incomplete corrective actions
- Number of corrective actions taken without having been recorded in a designated form

A current version of this document is available to all staff and under version control on the corporate document control system.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 349

6. Appendices

- Not applicable.

7. Change history

Date	Version	Created by	Description of change
22-JAN-2014	0.1	Rodrigo Ricci	Document creation
11-JUN-2014	1.0	Matthew Engler	Updated document format and grammar.
23-AUG-2014	2.0	Matthew Engler	Added section 3.3.3, Identifying Risk Owners
24-SEP-2014	3.0	Matthew Engler	Added a reference document
15-MAR-2016	4.0	Matthew Engler	Aligned risk scales with enterprise risk framework

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 350

stefanini
POWERING YOUR BUSINESS

PROCEDURE FOR RISK TREATMENT PLAN

Information Security Management System



Code:	ISMS-020
Version:	3.0
Date of version:	24-SEP-2014
Updated by:	Matthew Engler
Approved by:	Washington Souza
Confidentiality level:	Internal Use

Table of contents

1. PURPOSE, SCOPE AND USERS 3
2. REFERENCE DOCUMENTS 3
3. DESCRIPTION 3
3.1. RISKS TO BE TREATED 3
3.2. RISKS TREATMENT 3
3.3. GENERAL PRIORITIES 4
3.4. CONSIDERATIONS ON RESOURCES 4
3.5. TREATMENT DETAIL 4
4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 4
5. DOCUMENT MANAGEMENT 5
6. APPENDICES 5
7. CHANGE HISTORY 5

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 352

1. Purpose, scope and users

The purpose of this document is to describe the procedure to plan and deal with risk treatments.

The users of this document are personnel responsible for the conducting of risk assessments for the organization.

2. Reference Documents

Documents associated or linked are listed below:

- ISO/IEC 27001 standard, 6.1.1, 6.1.2, 6.1.3, 8.3
- ISMS-001 Policy, Information Security
- ISMS-019 Procedure, Risks Analysis
- Risks, Assets and Classification Spreadsheet
- Asset Valuation_Risk Treatment_Owners {year} (xlsx)

3. Description

3.1. Risks to be treated

Based upon the established Risk Management Methodology, the Top Management Representative considers as acceptable all risks lower or equal to the “Significant” level. The risks higher than such level are considered unacceptable, having to be mitigated, transferred or eliminated.

Management actions deemed appropriate for each of the risks considered unacceptable are detailed below, along with the controls found in Annex A of ISO / IEC 27001.

The risks to be treated are detailed on the Risk, Assets and Classification spreadsheet.

3.2. Risks Treatment

Stefanini has established as policy that risks deemed unacceptable must be appropriately treated, considering the following treatment options:

- Mitigate
- Eliminate
- Accept
- Transfer

Stefanini has come to the following decisions and considerations:

1. No risks can be adequately transferred.
2. It´s been observed that it is not possible to avoid risks to be treated when they are associated with critical assets and the threats cannot be eliminated.
3. According to the Risk Analysis Methodology, no risk higher than the acceptable will be accepted.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 353

4. Implementation of all necessary controls to mitigate risks and achieve a residual risk score lower than what is considered not acceptable.

Risk owners will formally approve the information security risk treatment plan and accept the residual information security risks. This approval may be through the Top Management Review, email, or other system where the approval is recorded.

The implementation of the selected controls is executed by the Information Security department and the Security Committee. The managers must require compliance with established ISMS policies and procedures. The responsible areas for carrying out the implementation of the controls are detailed in each place.

3.3. General priorities

The following items are established as priority:

1. Implementation of ISO/IEC 27002:2013 essential or good practices controls.
2. Implementation of staff qualification activities.
3. Implementation of controls for the identification and management of security incidents.
4. Implementation of controls associated to the identified unacceptable risks.
5. Implementation of the necessary metrics and indicators to determine the effectiveness of the implemented controls and thus verify the Information Security Management System effectiveness for the mitigation of the unacceptable risks.

3.4. Considerations on resources

In order to put the proposed treatment plan into practice, Stefanini will determine the necessary Human Resources and related budget requirements.

3.5. Treatment detail

The risks considered unacceptable are detailed and must be treated properly. The established treatment action is detailed for each one of the risks. For the mitigation cases, the controls to be implemented are indicated, as well as the associated roles and responsibilities, available resources and priority.

Please refer to the Risk, Assets and Classification spreadsheet.

4. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Control for record protection	Retention time
Risks, Assets and Classification	ISMS Portal	Information Security Manager or someone designated by him	Information Security Manager or someone designated by him is authorized to edit data	2 years

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 354

5. Document management

The owner of this document is the Information Security Manager, who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

- Number of assets
- Number of threats
- Number of threats by asset
- Number of risks by asset
- Number of initiated corrective actions
- Number of incomplete corrective actions
- Number of corrective actions taken without having been recorded in a designated form

A current version of this document is available to all staff and under version control on the corporate document control system.

6. Appendices

- Not applicable

7. Change history

Date	Version	Created by	Description of change
22-JAN-2014	1.0	Rodrigo Ricci	Document creation
23-AUG-2014	2.0	Matthew Engler	Added formal acceptance of risk treatment plan; Record location
24-SEP-2014	3.0	Matthew Engler	Added a Reference Document

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 355

CLEAR DESK AND CLEAR SCREEN POLICY

Information Security Management System



Code:	ISMS-022
Version:	1.0
Date of version:	22-JAN-2014
Created by:	Larissa Longo
Approved by:	Washington Souza
Confidentiality level:	Internal Use

Table of contents

1. PURPOSE, SCOPE AND USERS 3

2. REFERENCE DOCUMENTS 3

3. DESCRIPTION 3

3.1. WORKPLACE PROTECTION 3

3.1.1. Clear desk policy 3

3.1.2. Clear screen policy 3

3.2. PROTECTION OF SHARED FACILITIES AND EQUIPMENT 3

4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 4

5. DOCUMENT MANAGEMENT 4

6. APPENDICES 4

7. CHANGE HISTORY 4

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 357

1. Purpose, scope and users

The purpose of this document is to define rules to prevent unauthorized access to information in workplaces, as well as to shared facilities and equipment, via unattended methods.

This policy applies to Stefanini Employees, sub-contractors, consultants, business associates, and other workers at Stefanini, including all personnel affiliated with third parties and subsidiaries on the Stefanini infrastructure (collectively “User(s)”).

2. Reference documents

Documents associated or linked are listed below:

- ISO/IEC 27001 standard, A.11.2.8, A.11.2.9.
- ISMS-001 Policy, Information Security

3. Description

All information classified as "Internal use," "Restricted" and "Confidential" as specified in the Information Classification Policy are regarded as sensitive in this Clear Desk and Clear Screen Policy.

3.1. Workplace protection

3.1.1. Clear desk policy

If the authorized person is not at his/her workplace, all paper documents, as well as data storage media labeled as sensitive, must be removed from the desk or other places (printers, fax machines, photocopiers, etc.) to prevent unauthorized access.

Such documents and media must be stored in a secure manner in accordance with the Information Classification Policy.

3.1.2. Clear screen policy

If the authorized person is not at his/her workplace, all sensitive information must be removed from the screen, and access must be denied to all systems for which the person has authorization.

The clear screen policy is implemented by logging out of all systems or locking the screen with a password. All desktop and portable computers will be configured to auto-lock within 15 minutes of inactivity.

3.2. Protection of shared facilities and equipment

Documents containing sensitive information must immediately be removed from printers, fax and copy machines.

When receiving and distributing mail, the following must be followed:

- Mail may only be received via an attended entrance by the appropriate person (e.g. receptionist)
- Or via a secured Shipping / Receiving area

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 358

Shared fax machines as listed on the asset inventory should not be used for the reception of Confidential or Restricted information.

Unauthorized use of printers, photocopiers, scanners and other shared equipment for copying listed on the asset inventory is prevented by either locking the equipment in a facility, placing the equipment in a secured facility or through the use of a PIN number or password.

4. Managing records kept on the basis of this document

- Not applicable

5. Document management

The owner of this document is the Information Security Manager, who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria must be considered:

- number of incidents related to misuse of passwords by unauthorized persons
- number of incidents related to inadequate handling of passwords or access

A current version of this document is available to all staff and under version control on the corporate document control system.

6. Appendices

- Not applicable

7. Change history

Date	Version	Created by	Description of change
22-JAN-2014	1.0	Larissa Longo	Document creation

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 359

INCIDENT MANAGEMENT PROCEDURE

Information Security Management System



Code:	ISMS-023
Version:	3.0
Date of version:	25-AUG-2020
Created by:	Licsileth Palma
Approved by:	Washington Souza
Confidentiality level:	Internal Use

Table of contents

1. PURPOSE, SCOPE AND USERS 3
2. REFERENCE DOCUMENTS 3
3. DESCRIPTION 3
3.1 INCIDENT MANAGEMENT 3
3.1.1 RECEIPT AND CLASSIFICATION OF INCIDENTS, WEAKNESSES AND EVENTS 4
3.1.2 TREATMENT PROCESS FOR SECURITY WEAKNESSES OR EVENTS 4
3.1.3 TREATING MINOR INCIDENTS 5
3.1.4 TREATING MAJOR INCIDENTS 5
3.1 LEARNING FROM INCIDENTS 5
3.2 DISCIPLINARY ACTIONS 5
3.3 COLLECTION OF EVIDENCE 5
4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 5
5. DOCUMENT MANAGEMENT 6
6. APPENDICES 6
7. CHANGE HISTORY 6

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 361

1. Purpose, scope and users

The purpose of this document is to ensure quick detection of security events and weaknesses, and quick reaction and response to security incidents.

This policy applies to Stefanini Employees, sub-contractors, consultants, business associates, and other workers at Stefanini, including all personnel affiliated with third parties and subsidiaries on the Stefanini infrastructure (collectively “User(s)”).

2. Reference documents

Documents associated or linked are listed below:

- ISO/IEC 27001 standard, 10.1, A.16.1.
- ISMS-001 Policy, Information Security
- ISMS-009 Procedure, Corrective and preventive actions
- ISMS-034 List of Legal, regulatory and other requirements

3. Description

3.1 Incident management

An information security incident is a "single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security" (ISO/IEC 27000:2009).

Examples of possible security incidents include:

Help Desk or user

- Continuous lock of password;
- Pop up on the user’s Internet browser;
- Notice of database modifications;
- Release of e-mails blocked with an unrelated business subject;
- Station restarting by itself;
- Slowness in multiple workstations simultaneously;

Database

- Attempt to connect to the database from unknown user / ip.
- Excessive numbers of connections to the databases;

Servers

- Slowness on server;

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 362

- Suspected virus;
- Accumulation of email in queue;
- Server restarting continuously;
- Snapshot volume growth of data;

Telecom

- Access unknown or unusual network connections coming from suspicious regions;
- Heavy traffic on the LAN.

Facilities

- Theft of a computer or hard drive;
- Unauthorized visitor within the office.

Note: For Stefanini Colombia, the complementary procedure to be used is **Gestión de Incidentes de Seguridad de la Información PC-SI-01.**

3.1.1 Receipt and classification of incidents, weaknesses and events

Each employee, supplier or other third party who is in contact with information and/or systems of Stefanini must report any system weakness, incident or event which could lead to a possible security incident in the following way:

1. All information and communication technology-related security events must be reported to Information Security Team.
2. All facility-related security events (including physical theft) must be reported to Human Resources, Facility Management or the Information Security Team.
3. All other security events (e.g. systemic problems, process failures, etc..) must be reported to the Information Security Manager.

Incidents, weaknesses and events (collectively “Security Events”) must be reported as soon as possible, by phone, by web or in person. These Security Events should be submitted via the Service Desk ticketing system, whenever possible.

Security Events will be classified in the following way:

a) Security Weakness – no incident occurred, but the event related to a system, process or organization may trigger the occurrence of an incident in the future.
b) Minor Incident – an incident which cannot significantly impact confidentiality or integrity of information, and cannot cause long-term unavailability.
c) Major Incident – an incident which can incur significant damage due to loss of confidentiality or integrity of information, or may cause an interruption in the availability of information and/or processes for an unacceptable period of time.

3.1.2 Treatment process for security weaknesses or events

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 363

The Analyst who receives the information about a security weakness or event analyzes the information, establishes the cause and, if necessary, suggests preventive and corrective action. This may be communicated via either e-Mail or the Service Desk ticketing system.

3.1.3 Treating minor incidents

If a minor Incident was reported, the person who received the information must take the following steps:

1. Take measures to contain the incident
2. Analyze the cause of the incident
3. Take corrective actions to eliminate the cause of the incident
4. Inform the proper persons who were involved in the Incident about the incident treatment process

The Analyst who receives information about a minor Incident must be submitted as a Normal Incident through the Service Desk ticketing system.

3.1.4 Treating major incidents

In the case of major incidents that could disrupt activities for an unacceptable period of time, an Incident Response Plan as part of the Business Continuity Plan is invoked.

Major Incidents must be submitted as a Critical Incident through the Service Desk ticketing system.

3.1 Learning from incidents

The Information Security Manager must review all minor Incidents every three months, and enter recurring ones or those which may turn into major Incidents on the next occasion, as a Problem record.

The Information Security Manager must analyze each Problem record (identifying type, relatedness, and cost of Incident) and, if necessary, suggest preventive or corrective actions.

3.2 Disciplinary actions

The Information Security Manager must invoke a disciplinary process for each violation of security rules.

3.3 Collection of evidence

The Top Management Representative or Information Security Manager will define the rules on how to identify, collect and preserve evidence that will be accepted as evidence in legal and other proceedings.

4. Managing records kept on the basis of this document

Record name	*Storage location*	*Person responsible for storage*	*Controls for record protection*	*Retention time*
Problem Record	Service Desk System	Service Desk	Only personnel with authorized Analyst access may modify the records.	A minimum of 2 years following closure of

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 364

				the Problem.
Rules for identifying, collecting and preserving evidences	Shared folder on the intranet or portal	Top Management Representative or Information Security Manager	Only Top Management Representative or Information Security Manager has the right to edit and publish the rules	Indefinitely

Only The Top Management Representative or Information Security Manager can grant other employees access to the records.

5. Document management

The owner of this document is the Information Security Manager, who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria must be considered:

- number of incidents related to misuse of passwords by unauthorized persons
- number of incidents related to inadequate handling of passwords

A current version of this document is available to all staff and under version control on the corporate document control system.

6. Appendices

- Not applicable

7. Change history

Date	Version	Created by	Description of change
22-JAN-2014	1.0	Rodrigo Ricci	Document creation
1-SEP-2015	2.0	Matthew Engler	Clarified physical theft Incidents
25-AUG-2020	3.0	Licsileth Palma	The use of PC-SI-01 procedure is included for Colombia.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 365

SUPPLIER SECURITY POLICY

Information Security Management System



Code:	ISMS-024
Version:	3.0
Date of version:	25-AUG-2020
Created by:	Licsileth Palma
Approved by:	Washington Souza
Confidentiality level:	Internal Use

Table of contents

1. PURPOSE, SCOPE AND USERS 3

2. REFERENCE DOCUMENTS 3

3. DESCRIPTION 3

3.1. REQUIREMENTS OF PROJECT SPONSORING ORGANIZATION 3

3.2. REQUIREMENTS OF THE SUPPLIER 4

3.3. TRAINING AND AWARENESS 4

3.4. MONITORING AND REVIEW 4

3.5. CHANGES OR TERMINATION OF SUPPLIER SERVICES 4

3.6. REMOVAL OF ACCESS RIGHTS / RETURN OF ASSETS 5

4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 5

5. DOCUMENT MANAGEMENT 5

6. APPENDICES 5

7. CHANGE HISTORY 6

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 367

1. Purpose, scope and users

The Supplier Security Policy describes the Information Security requirements of suppliers that engage with Stefanini.

This document is applied to all suppliers and partners who have the ability to influence confidentiality, integrity and availability of data entrusted to Stefanini.

This policy applies to any use of suppliers by Stefanini independent of where data may be hosted.

2. Reference documents

Documents associated or linked tare listed below:

- ISO/IEC 27001 standard, 4.1, 4.2, 7.4, A.5.1.1, A.7.1.2, A.7.2.2, A.7.3.1., A.15
- ISMS-001 Policy, Information Security
- ISMS-011 Policy, Change management
- ISMS-013 Procedure, Training and Awareness
- ISMS-019 Procedure, Risks Identification and Assessment
- ISMS-021 Procedure, Risk Treatment Plan
- ISMS-049 Standard, Supplier security
- Relationship Processes (ISO 20000)

3. Description

3.1. Requirements of Project Sponsoring Organization

The Supplier's Sponsoring Organization must first establish that its project is an appropriate one for Stefanini's objectives, prior to engaging any additional infrastructure teams within Stefanini or Suppliers external to the company. The person/team wanting to use the supplier service must confirm that the supplier chosen complies with this policy. If a Business Function is to be outsourced, it must be evaluated against the following:

- The requester must go through the supplier engagement process (refer to Supplier Management ISO 20000. For Stefanini Colombia, refer to PC-CO-05 Selección de Proveedores/Aliados) with the ICT Management to ensure affected parties are properly engaged.
- In the event that Stefanini data or applications are to be manipulated by, or hosted at, a supplier's service, the supplier's sponsoring organization must have written, explicit permission from the data/application owners. A copy of this permission must be provided to the Information Security Manager.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 368

- If the supplier provides confidential information to Stefanini the supplier's sponsoring organization is responsible for ensuring that any obligations of confidentiality are satisfied. This includes information contained in the supplier's application (if applicable). Stefanini's legal services department must be contacted for further guidance if questions about third-party data arise. Projects that do not meet these criteria may not be deployed to a supplier.

3.2. Requirements of the Supplier

The Information Security Team has created an associated document, entitled *ISMS-049 Standard, Supplier security* that sets forth the minimum security requirements for data hosting suppliers subject to this policy. The supplier must demonstrate compliance with these Standards in order to be considered for use.

The supplier engagement process includes the Information Security Team evaluation of security requirements.

The Information Security Manager may request that additional security measures be implemented, depending on the nature of the project. The Information Security Management Team may change the requirements over time, and the supplier is expected to comply with these changes or document exceptions.

Suppliers that do not meet these requirements may not be used for Stefanini projects.

Supplier contracts should allow for an independent audit of security controls by Stefanini or a third party auditor.

3.3. Training and awareness

Based upon the supplier's function, the Information Security Team may decide that employees of the suppliers or partners need security awareness and training. The Top Management Representative, Information Security Manager or Department Manager is responsible to provide all the training for those employees.

3.4. Monitoring and review

Contract owner must regularly check and monitor the level of service and fulfillment of security clauses by suppliers or partners, reports and records created by the supplier/partner. This review must include:

- Service Level Agreement Performance;
- Security Incidents related to the supplier;
- Vendor Corrective Action status;
- Security KPIs defined (if applicable);

All the security incidents related to the partner's/supplier's job must be forwarded immediately to the Information Security Manager.

3.5. Changes or termination of supplier services

If a Contract owner proposes changes or termination of the contract, the Global Information Security office must be notified to ensure access rights and risks are properly evaluated.

Note: For Stefanini Colombia, it will be carried out as established in procedure PC-CO-04 Evaluación de Proveeores.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 369

3.6. Removal of access rights / return of assets

When the contract is changed or terminated, the access rights for employees of partners/suppliers must be removed according to the Access Control Policy.

Further, when the contract is changed or terminated, the contract owner must make sure all the equipment; software or information in electronic or paper form is returned.

4. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
Contracts with suppliers and partners	Electronic: Shared Drives; Paper: Locked Cabinets	Suppliers control area	Only area people has access to the cabinet	5 years after the termination of the contract
Records of monitoring and review	Per *Supplier Management Process*	Contract owner	Only users with a need to know may access as determined by the contract owner or legal.	2 years

5. Document management

The owner of this document is the Suppliers Control area (For Stefanini Colombia, Purchasing Area), who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria must be considered:

- number of incidents related to misuse of passwords by unauthorized persons
- number of incidents related to inadequate access

A current version of this document is available to all staff and under version control on the corporate document control system.

6. Appendices

- Not applicable

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 370

7. Change history

Date	Version	Created by	Description of change
01-APR-2014	1.0	Matthew Engler	Document creation
23-AUG-2014	2.0	Matthew Engler	Added contract requirement language; Added explicit review criteria
25-AUG-2020	3.0	Licsileth Palma	The use of procedures PC-CO-03 Selección de Proveedores/Aliados and PC-CO-04 Evaluación de Proveedores are included for Colombia

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 371

EQUIPMENT MAINTENANCE PROCEDURE

Information Security Management System



Code:	ISMS-025
Version:	2.0
Date of version:	25-AUG-2020
Created by:	Licsileth Palma
Approved by:	Washington Souza
Confidentiality level:	Internal Use

Table of contents

1. PURPOSE, SCOPE AND USERS 3
2. REFERENCE DOCUMENTS 3
3. DESCRIPTION 3
3.1. MAINTENANCE PLANNING 3
3.2. MAINTENANCE 3
4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 4
5. DOCUMENT MANAGEMENT 4
6. APPENDICES 4
7. CHANGE HISTORY 4

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 373

1. Purpose, scope and users

This procedure indicates how to plan and perform maintenance for the main infrastructure equipment within the scope of ISMS.

Users of this document are the Information Security Manager.

2. Reference documents

Documents associated or linked are listed below:

- ISO/IEC 27001 standard, A.11.2.4.
- ISMS-001 Policy, Information Security
- Maintenance plan
- Equipment Maintenance Form

3. Description

3.1. Maintenance Planning

The Information Security Manager and the asset owners are responsible to:

- Annually, define what equipment can affect the ISMS and need maintenance
- Prepare a Maintenance Plan with the planned time and records needed
- Check, during the year, if there is any other equipment that needs maintenance and review the plan.

3.2. Maintenance

The Administrative area follows the Maintenance Plan and defines the provider that will make the activity.

The providers must follow the Information Security policies.

The records are kept by Administrative area and a copy is accessible for the Information Security Manager.

If rescheduling is required, then the Administrative area, the Information Security Manager and all affected parties will agree on a revised schedule. This revised schedule will be documented.

In maintenance situation where the plan was not followed or equipment was not functioning properly following maintenance, an Incident must be recorded in the proper tool.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 374

4. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
Maintenance records	Administrative area folder or cabinet Service Desk ticketing system	Administrative area	Administrative area or Information Security Manager can access the records	Twelve months of historical

5. Document management

The owner of this document is the Information Security Manager, who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria must be considered:

- number of incidents detected
- maintenance Plan compliance

A current version of this document is available to all staff and under version control on the corporate document control system.

6. Appendices

- Not applicable

7. Change history

Date	Version	Created by	Description of change
22-JAN-2014	1.0	Luiz Robson	Document creation
25-AUG-2020	2.0	Licsileth Palma	Reference documents update

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 375

INFORMATION TRANSFER POLICY

Information Security Management System



Code:	ISMS-027
Version:	3.0
Date of version:	25-AUG-2020
Created by:	Licsileth Palma
Approved by:	Washington Souza
Confidentiality level:	Internal Use

Table of contents

1. PURPOSE, SCOPE AND USERS 3

2. REFERENCE DOCUMENTS 3

3. DESCRIPTION 3

3.1. ELECTRONIC COMMUNICATION CHANNELS 3

3.2. RELATIONS WITH EXTERNAL PARTIES 3

3.3. DATA HANDLING 4

4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 5

5. DOCUMENT MANAGEMENT 5

6. APPENDICES 5

7. CHANGE HISTORY 5

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 377

1. Purpose, scope and users

The purpose of this document is to ensure the security of information and software when they are exchanged within or outside the organization.

This policy applies to Stefanini Employees, sub-contractors, consultants, business associates, and other workers at Stefanini, including all personnel affiliated with third parties and subsidiaries on the Stefanini infrastructure (collectively “User(s)”).

2. Reference documents

Documents associated or linked are listed below:

- ISO/IEC 27001 standard, A.8.2.3, A.8.3.3, A.13.2.1, A.13.2.2.
- ISMS-001 Policy, Information Security
- ISMS-024 Policy, Supplier security
- ISMS-028 Policy, Information Classification and Handling

3. Description

3.1. Electronic communication channels

Stefanini's information may be exchanged through the following electronic communication channels: e-mail, download of files from the Internet, transfer of data via FTP (SFTP preferred; needs to be authorized by Infrastructure and Support Departments), telephones and portable media (i.e CD or DVD need to be authorized by Infrastructure and Support Departments).

Infrastructure and Support Departments determines the communication channel that may be used for each type of information, and possible restrictions regarding permissions to use the communication channels.

In addition to controls prescribed by the *ISMS-028 Policy, Information Classification and Handling*, additional controls for each type of data and communication channel can be addressed based on risk assessment results.

3.2. Relations with external parties

External parties include various service providers, companies for hardware and software maintenance, companies handling transactions or data processing, clients, etc.

Before exchanging information and/or software with any external party, an agreement must be signed, according to *ISMS-024 Policy, Supplier security* or contractual requirements. The agreement may be in paper or electronic form (e.g. agreeing to general terms and conditions) and must contain clauses in line with the risk assessment, including at least the following:

- method of identification of the other party
- authorizations to access information
- ensuring non-repudiation

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 378

- incident response
- labeling and handling sensitive information
- copyright

Agreements with external parties must be drawn up according to the *ISMS-024 Policy, Supplier security*.

Agreements with clients must be made as contractually agreed.

3.3. Data Handling

- Public
  - No special requirements
- Internal Use
  - Electronic transmissions must comply with marking/labelling/identification requirements.
  - May be transmitted via company provided electronic networks.
  - Facsimile transmissions require destination verification (phone number)
  - When files are exchanged with external parties via services such as FTP, instant messaging, etc., they should be password protected
  - Encryption is recommended on transmissions through public networks (Internet).
  - If physically sent outside the organization, the document must be sent as registered mail or through government postal service.
- Confidential
  - Electronic transmissions must comply with marking/labelling/identification requirements.
  - May be transmitted via company provided electronic networks.
  - Facsimile transmissions require destination verification (phone number)
  - When files are exchanged with external parties via services such as SFTP, instant messaging, etc., they must be encrypted and password protected
  - Encryption is recommended on transmissions through public networks (Internet).
  - If physically sent outside the organization, the document must be mailed with a return receipt service or delivery tracking mechanism.
- Restricted
  - Electronic transmissions must comply with marking/labelling/identification requirements.
  - May be transmitted via company provided electronic networks.
  - Facsimile transmissions require destination verification (phone number)
  - When files are exchanged with external parties via services such as SFTP, instant messaging, etc., they must be encrypted and password protected.
  - Encryption is required on transmissions through public networks (Internet).
  - If physically sent outside the organization, the document must be mailed with a return receipt service / tracking.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 379

Note: For Stefanini Colombia, the complementary procedure to be used is Instructivo Transferencia de la Información IN-SI-03.

4. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
Decisions about the communication channels used for specific types of information, restrictions, forbidden activities – electronic form	ISMS portal	Infrastructure and Support Department	Once created, the record cannot subsequently be changed	3 years

5. Document management

The owner of this document is the Infrastructure and Support Departments, who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria must be considered:

- number of incidents related to misuse of passwords by unauthorized persons
- number of incidents related to inadequate transfer of information

A current version of this document is available to all staff and under version control on the corporate document control system.

6. Appendices

- Not applicable

7. Change history

Date	Version	Created by	Description of change
08-APR-2014	1.0	Luiz Robson; Matthew Engler	Document creation
04-SEP-2015	2.0	Matthew Engler	Clarified file exchange requirements with external parties.
25-AUG-2020	3.0	Licsileth Palma	The use of the instruction IN-SI-03 is included for Colombia

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 380

INFORMATION CLASSIFICATION AND HANDLING POLICY

Information Security Management System



Code:	ISMS-028
Version:	4.0
Date of version:	04-SEP-2015
Updated by:	Matthew Engler
Approved by:	Washington Souza
Confidentiality level:	Internal Use

Table of contents

1. PURPOSE, SCOPE AND USERS 3
2. REFERENCE DOCUMENTS 3
3. DESCRIPTION 3
3.1. CLASSIFIED INFORMATION 3
3.1.1. Tasks and responsibilities 3
3.1.2. Classification of information 4
3.1.2.1. Classification criteria 4
3.1.2.2. Confidentiality levels 5
3.1.2.3. List of Authorized Persons 6
3.1.2.4. Reclassification 6
3.1.3. Information labeling 6
3.1.4. Handling classified information 6
3.2. MARKING AND LABELING 7
3.3. STORAGE AND DESTRUCTION 7
3.4. RETENTION 8
3.5. INFORMATION SHARING (OUTSIDE OF STEFANINI) 9
3.6. TRANSMISSION 9
4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 9
5. DOCUMENT MANAGEMENT 10
6. APPENDICES 10
7. CHANGE HISTORY 10
APPENDIX A – EMAIL CLASSIFICATION 11

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 382

1. Purpose, scope and users

The *Information Classification and Handling Policy* is intended to help Stefanini Users determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed inside or outside of Stefanini without proper authorization. Information stored on or originating from Stefanini systems is the property of Stefanini or its customers and its integrity is crucial to the success of the company. Stefanini information must be protected from unauthorized access, modification, disclosure and destruction whenever it is transferred or stored. Information must be classified to establish, formally and consistently, the appropriate precautions that must be taken.

This document is applied to all types of information, regardless of the form – paper or electronic documents, applications and databases, people's knowledge, etc.

This policy applies to Stefanini Employees, sub-contractors, consultants, business associates, and other workers at Stefanini, including all personnel affiliated with third parties and subsidiaries on the Stefanini infrastructure (collectively "User(s)").

2. Reference documents

Documents associated or linked are listed below:

- ISO/IEC 27001 standard, A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.9.4.1
- ISMS-001 Policy, Information Security
- ISMS-003 Statement of Applicability
- ISMS-010 Policy, Acceptable use
- ISMS-019 Procedure, Risks Identification and Assessment
- ISMS-021 Procedure, Risk Treatment Plan
- ISMS-023 Procedure, Incident Management
- ISMS-027 Policy, Information Transfer
- ISMS-034 List of Legal, regulatory and other requirements
- ISMS-037 Policy, Media Sanitization and Disposal
- ISMS-041 Policy, Communications and Operations Security

3. Description

3.1. Classified information

3.1.1. Tasks and responsibilities

- All data created by Stefanini or legally acquired through third parties will be classified by the information owner as Public, Internal Use, Confidential or Restricted.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 383

- Information, in any form, will be handled in accordance with the Data Handling Standards defined below for the appropriate classification. Data Handling includes the transmission, storage, labelling, sharing, and destruction of data.
- Internal Use, Confidential and Restricted information will not be disclosed or used by any other person without prior authorization.
- Users will respect the confidentiality and privacy of individuals whose records they access, observe ethical restrictions that apply to the information they access, and abide by applicable laws and policies with respect to accessing, using, or disclosing information.
- Confidential and Restricted information must remain within Stefanini facilities, including co-locations, or within the possession of an authorized third party and must be protected from unauthorized access.
- Non-Stefanini Personnel having access to Stefanini confidential and restricted information must be bound by a mutual non-disclosure agreement.
- Where required, procedural controls are mandated to mitigate risk. This also includes controls from third party standards and guidelines.
- All data assets provided by a customer will be considered Confidential, unless otherwise indicated. The Asset Owner will be the Stefanini manager responsible for the customer relationship.

Tasks and responsibilities for information management are the following:

Task	*Responsibility*
1. Entering the information asset in the Inventory of Assets	Infrastructure, HR, Governance, Administrative
2. Classification of information	Asset owner
3. Information labeling	Asset owner
4. Information handling	Persons with access rights in accordance with this Policy

If information assets are received from outside the organization, the asset owner is responsible for its classification in accordance with the rules prescribed in this Policy.

3.1.2. Classification of information

3.1.2.1. Classification criteria

The level of confidentiality is determined based on the following criteria:

- Value of information – based on impacts assessed during risk assessment
- Sensitivity and criticality of information – based on the highest risk calculated for each information asset during the risk assessment
- Legal and contractual obligations – based on the *ISMS-034 List of Legal, regulatory and other requirements*

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 384

3.1.2.2. Confidentiality levels

All information must be classified into confidentiality levels.

Confidentiality level	*Labeling*	*Classification criteria*	*Access restriction*
Public	(unlabeled)	Data could be made public without any implications for the company (i.e. the data is not confidential). Data integrity is not vital. Loss of service due to malicious attacks is an acceptable danger.	Information can be disclosed or disseminated without any restrictions on content, audience or time of publication. Disclosure or dissemination of the information must not violate any applicable laws or regulations, such as privacy rules. Modification must be restricted to individuals who have been explicitly approved by information owners to modify that information, and who have successfully authenticated themselves to the appropriate computer system.
Internal use	INTERNAL USE	External access to this data is to be prevented, but should this data become public, the consequences are not critical (e.g. the company may be publicly embarrassed). Internal access is selective. Data integrity is important but not vital.	Information can be disclosed or disseminated by its owner to appropriate members of Stefanini, partners and other individuals, as appropriate by information owners without any restrictions on content or time of publication.
Confidential	CONFIDENTIAL	Data in this class is confidential within the company and protected from external access. If such data were to be accessed by unauthorized persons, it could influence the company's operational effectiveness, cause an important financial loss, provide a significant gain to a competitor or cause a major drop in customer confidence. Data integrity is vital.	Information can be disclosed or disseminated by its owner to appropriate members of Stefanini, partners and other individuals, as authorized by information owners. Information is subject to controls on access and ensuring proper protections are in place.
Restricted	RESTRICTED	Unauthorized external or internal access to this data would be critical to the company. Data integrity is vital. The number of people with	Only those who explicitly need access must be granted it, and only to the least degree in order to do their work (the 'need to

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 385

		access to this data should be very small. Very strict rules must be adhered to in usage of this data.	know' and 'least privilege' principles).

The basic rule is to use the lowest confidentiality level ensuring an appropriate level of protection, in order to avoid unnecessary protection costs.

3.1.2.3. List of Authorized Persons

Access to information classified as "Confidential" or "Restricted" must be authorized by the information owner. The Information Owner may define a list of roles or job functions which may access the information.

The same rule applies to the confidentiality level "Internal use" if people outside the organization will have access to such a document.

3.1.2.4. Reclassification

Asset owners must review the confidentiality level of their information assets every two years and assess whether the confidentiality level should be changed.

3.1.3. Information labeling

Confidentiality levels are labeled in the following way:

- Paper / Electronic documents – Please refer to section 3.2.
- Digital media – the confidentiality level of digital media (e.g. information contained within a database) will be maintained by the Information Security department within the *Risk, Assets and Classification* list.
- All Other Media – the confidentiality level of all other media (e.g. information on a whiteboard) will be maintained by the Information Security department within the *Risk, Assets and Classification* list.

3.1.4. Handling classified information

All persons accessing classified information must follow the rules listed. The Top Management Representative or Head of Information Security must initiate disciplinary action each time the rules are breached or if the information is communicated to unauthorized persons. Each incident related to handling classified information must be reported in accordance with the Incident Management Procedure.

Information assets may be taken off-premises only after obtaining authorization in accordance with the *ISMS-010 Policy, Acceptable use*.

The method for secure erasure and destruction of media is prescribed in the document Operating *ISMS-041 Policy, Communications and Operations Security / ISMS-037 Media Sanitization and Disposal Policy*

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 386

3.2. Marking and Labeling

Original information/data is to be visibly and conspicuously marked/labelled with the appropriate Classification. Duplications of original information/data must additionally be marked with identifying information of the parties with whom it is intended to be shared.

- Public
  - No special marking required
- Internal Use - Marked in one of the following ways:
  - Each page/part of information/work product marked with appropriate Sensitivity Classification.
  - A formal statement at the beginning of the document may be used.
- Confidential – Marked with at least one of the following:
  - Each page/part of information/work product marked with appropriate Sensitivity Classification.
  - A formal statement at the beginning of the document may be used.
  - Indicated on the front of the cover or envelope carrying such a document
- Restricted – Marked with at least one of the following:
  - Each page/part of information/work product marked with appropriate Sensitivity Classification.
  - A formal statement at the beginning of the document may be used.
  - Indicated on the front of the cover or envelope carrying such a document

3.3. Storage and Destruction

All information / data is to be stored and destroyed properly according to Classification. Please refer to the *ISMS-037 Policy, Media Sanitization and Disposal* for destruction requirements.

- Public
  - No special requirements
- Internal Use
  - Work area:
    - Information/data may be left on work area during work hours but needs to be secured after hours.
    - Electronic information may be left on a computer hard drive or portable media. the screen must be automatically locked after 15 minutes of inactivity
  - Destruction:
    - Use prudent disposal methods that will prevent further distribution.
    - Please refer to the *ISMS-037 Policy, Media Sanitization and Disposal* for destruction requirements.
- Confidential
  - Work area:

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 387

        - Information/data may be left on work area during work hours but needs to be secured after hours.
        - Electronic information may be left on a computer hard drive or portable media. the screen must be automatically locked after 15 minutes of inactivity
    - Destruction:
        - Use prudent disposal methods that will prevent further distribution.
        - Please refer to the *ISMS-037 Policy, Media Sanitization and Disposal* for destruction requirements.

- Restricted
    - Secured control area:
        - Keep information/work product out of sight from casual observation while in use during work hours.
        - Whenever information/work product is unattended, secure the area or practice a clean desk policy. The screen must be automatically locked after 15 minutes of inactivity
        - Secure after hours.
    - Non-secured control area:
        - Keep in possession and out of sight from casual observation while in use during work hours.
        - Keep securely locked in a storage compartment at all times.
    - Electronic storage:
        - Information must not be left on a personal computer hard drive unless it is encrypted.
        - Information must not be left on a company managed resource (e.g. file servers, corporate shared resources) unless password/access protected and/or encrypted.
        - Encryption recommended for information residing on database.
        - Information on portable media (diskettes, USB drives) must be password protected and/or encrypted.
    - Destruction:
        - Use prudent disposal methods that will prevent further distribution.
        - Please refer to the *ISMS-037 Policy, Media Sanitization and Disposal* for destruction requirements.

3.4. Retention

- Public
    - No special requirements
- Internal Use
    - Data must only be retained as long as required by business need or legal requirements. Please refer to the Record Retention Policy or as defined in Policy / procedure document.
- Confidential
    - Data must only be retained as long as required by business need or legal requirements. Please refer to the Record Retention Policy or as defined in Policy / procedure document.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 388

- Restricted
  - Data must only be retained as long as required by business need or legal requirements. Please refer to the Record Retention Policy or as defined in Policy / procedure document.

3.5. Information Sharing (outside of Stefanini)

See also *ISMS-027 Policy, Information Transfer*.

- Public
  - No special requirements
- Internal Use
  - Sharing requires permission of the owner or functional department who are the originators of the information/data.
- Confidential
  - Sharing requires permission of the owner or functional department who are the originators of the information/data.
  - Information/data of a unique or highly specific nature require cross-functional permission.
- Restricted
  - Sharing requires permission of the owner or functional department who are the originators of the information/data.
  - Information/data of a unique or highly specific nature require cross-functional permission.
  - Could require management and/or legal approval.
  - A distribution/retrieval log of recipients must be maintained by the owner if physically removed.
  - Any authorized disclosure must be made under conditions which impose on the receiving party an obligation to maintain the confidential nature of the information and appropriate restrictions on use and disclosure.
  - Cannot be shared without permission of client and must meet requirements and other restrictions as may be imposed by law.

3.6. Transmission

- Refer to *ISMS-027 Policy, Information Transfer*.

4. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
List of Authorized Persons with access to documents, where applicable	Together with the information where the confidentiality level is indicated	Information asset owner	The same as for the protection of information	The List must exist as long as the information itself exists

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 389

5. Document management

The owner of this document is the Information Security Manager, who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria must be considered:

- number of incidents related to misuse of passwords by unauthorized persons
- number of incidents related to inadequate handling of passwords

A current version of this document is available to all staff and under version control on the corporate document control system.

6. Appendices

- Appendix A – eMail Classification

7. Change history

Date	Version	Created by	Description of change
08-APR-2014	1.0	Luiz Robson; Matthew Engler	Document creation
28-AUG-2014	2.0	Matthew Engler	Added default classification for Customer data.
10-SEP-2014	3.0	Matthew Engler	Added eMail Classification
04-SEP-2015	4.0	Matthew Engler	Revised Data Marking requirements

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 390

Appendix A – eMail Classification

Communications sent via eMail will be classified / marked in the following ways. By default, all eMail is classified as INTERNAL USE:

- Public
  - If eMail is intended to be public information, the body of the eMail should indicate that the information is Public.
- Internal Use
  - By default, all eMail is considered Internal Use regardless of destination.
  - No special markings are required when sending to Internal users.
  - When sending to External users, a disclaimer (example below) shall be appended to each eMail.
- Confidential
  - eMail which is Confidential may be marked in one of two ways:
    - The word CONFIDENTIAL should proceed the subject line (Preferred).
    - A Confidential tag may be used through the eMail client, if available.
- Restricted
  - eMail which is Restricted shall be marked with the word RESTRICTED proceeding the subject line.

Example Disclaimer:

- The information transmitted is intended only for use by the addressee and may contain confidential and/or privileged material. Any review, re-transmission, dissemination or other use of it, or the taking of any action in reliance upon this information by persons and/or entities other than the intended recipient is prohibited. If you received this in error, please inform the sender and/or addressee immediately and delete the material.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 391

BRING YOUR OWN DEVICE – BYOD POLICY

Information Security Management System



Code:	ISMS-029
Version:	1.0
Date of version:	21-JAN-2014
Created by:	Luiz Robson
Approved by:	Washington Souza
Confidentiality level:	Internal Use

Table of contents

1. PURPOSE, SCOPE AND USERS 3

2. REFERENCE DOCUMENTS 3

3. DESCRIPTION 3

3.1. SECURITY RULES FOR USING BYOD 3

3.1.1. Company Policy 3

3.1.2. Who is allowed to use BYOD and for what 3

3.1.3. Which devices are allowed 3

3.1.4. Acceptable use 3

3.1.5. Special Rights 4

3.1.6. Security breaches 5

3.1.7. Training and awareness 5

4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 5

5. DOCUMENT MANAGEMENT 5

6. APPENDICES 5

7. CHANGE HISTORY 6

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 393

1. Purpose, scope and users

The purpose of this document is to define how Stefanini will retain control over its information while such information is being accessed through devices that are not owned by the organization.

This document is applied to all personally owned devices that have the ability to store, transfer or process any sensitive information from the Information Security Management System (ISMS) scope. Those devices include laptops, smart phones, tablets, USB memory sticks, digital cameras, etc. Such devices will be referred to as BYOD in this Policy.

This policy applies to Stefanini Employees, sub-contractors, consultants, business associates, and other workers at Stefanini, including all personnel affiliated with third parties and subsidiaries on the Stefanini infrastructure (collectively "User(s)").

2. Reference documents

Documents associated or linked are listed below:

- ISO/IEC 27001 standard, A.6.2.1, A.6.2.2, A.8.2.3, A.13.2.1
- ISMS-001 Policy, Information Security
- ISMS-028 Policy, Information Classification and Handling

3. Description

3.1. Security Rules for using BYOD

The rules in this Policy apply to all BYOD, whether they are used for work or for private use, or whether they are used within or outside of the organization's premises:

3.1.1. Company Policy

Stefanini supports widespread use of BYOD for work use – i.e. using such devices for performing work for the company.

The company data that is stored, transferred or processed on BYOD remains under the company's ownership, and the company retains the right to control such data even though it is not the owner of the device.

3.1.2. Who is allowed to use BYOD and for what

The Infrastructure and Support Department will create a list of job titles and/or persons who are allowed to use BYOD, together with the applications and databases they are allowed to access with their own devices.

3.1.3. Which devices are allowed

The Infrastructure and Support Departments will create / maintain a list of currently acceptable classes of devices (e.g. Smart Phones, Laptop, Tablet), which can be used as BYOD. The list will set forth the minimum-security settings for each device.

3.1.4. Acceptable use

For each BYOD, the following are mandatory:

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 394

- When using BYOD outside of the company premises, it must not be left unattended and, if possible, should be physically locked away
- When using BYOD in public places, the owner must take care that data cannot be read by unauthorized persons
- Patches and updates must be installed regularly
- When available, anti-software / anti-malware software must be installed and maintained in accordance with *ISMS-039, Anti-Virus / Anti-Malware Software Policy*.
- Classified information must be additionally protected according to the Information *ISMS-028 Policy, Information Classification and Handling*
- Describe in specific operational procedures:
    - How the backup of company information must be made
    - Which security software must be installed – e.g. anti-virus software, intrusion prevention, mobile device management software, etc.
    - The method of encryption that is to be used and for what
    - The method of authentication that is to be used
    - The secure method of connection to the company network

It is not allowed to do the following with BYOD:

- Allow access to anyone else except the employee who is the owner of the device
- Install applications that are not permitted
- Store illegal materials on the device
- Install unlicensed software
- Connect to unknown Wi-Fi networks
- Use Bluetooth without a clearly defined need
- Locally store passwords
- Locally store information, in accordance with the *ISMS-028 Policy, Information Classification and Handling*
- Transfer company data to other devices which are not allowed

3.1.5. Special Rights

Stefanini has the right to view, edit, and delete all company data that is stored, transferred or processed on BYOD.

The Infrastructure and Support Department is authorized to configure any BYOD according to this Policy and monitor its use.

Stefanini has the right to perform full deletion of all data on BYOD if it considers that necessary for the protection of the company data, without the consent of the device owner.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 395

3.1.6. *Security breaches*

All security breaches related to BYOD must be reported immediately to Information Security organization. Further, all weaknesses that have not yet become incidents must be reported through the same channels.

3.1.7. *Training and awareness*

The Human Resource area or the employee Manager is in charge of training new and existing employees on appropriate use of BYOD, as well as raising awareness about the most common threats.

4. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Control for record protection	Retention time
List of allowed users for BYOD and what they can access	ISMS Portal	Designated by Information Security Manager	Only the Designated by Information Security Manager can edit and publish new version of the List	List that is no longer valid must be archived for 2 years
List of acceptable BYOD devices and their settings	ISMS Portal	Designated by Infrastructure and Support Department.	Only the Designated by Infrastructure and Support Department can edit and publish new version of the List	List that is no longer valid must be archived for 2 years

5. Document management

The owner of this document is the Information Security Manager, who must check and, if necessary, update the document at least once a year. The Information Security Manager will review List of allowed users, List of acceptable devices, every 6 months.

When evaluating the effectiveness and adequacy of this document, the following criteria must be considered:

- number of incidents related to use of BYOD
- number of employees using BYOD without authorization

A current version of this document is available to all staff and under version control on the corporate document control system.

6. Appendices

- Not applicable

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 396

7. Change history

Date	Version	Created by	Description of change
22-JAN-2014	1.0	Luiz Robson	Document creation

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 397

stefanini
POWERING YOUR BUSINESS

MEASURING THE EFFECTIVENESS OF THE CONTROLS PROCEDURE

Information Security Management System



Code:	ISMS-030
Version:	2.0
Date of version:	22-SEP-2016
Created by:	Matthew Engler
Approved by:	Washington Souza
Confidentiality level:	Internal Use

Table of contents

1. PURPOSE, SCOPE AND USERS 3
1.1. RESPONSIBILITIES 3
1.2. DEFINITIONS AND ABBREVIATIONS 3
2. REFERENCE DOCUMENTS 3
3. DESCRIPTION 3
3.1. EFFECTIVENESS MEASUREMENT COMPLIANCE MEETINGS 3
3.2. OBJECTIVE MEASUREMENT PROCESS 4
3.3. METRICS AND INDICATORS 4
3.4. LIFECYCLE 4
3.5. INDICATORS REVIEW 4
4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 4
5. DOCUMENT MANAGEMENT 5
6. APPENDICES 5
6.1. METRICS 5
7. CHANGE HISTORY 8

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 399

1. Purpose, scope and users

The purpose of this document is to define the responsibilities, methodology and processes used by Stefanini to measure the effectiveness of implemented controls, and the degree of fulfillment of the objectives of selected control.

Users of this document are the employees responsible for control reviews within the organization.

1.1. Responsibilities

The Security Committee is responsible for the periodic review of the effectiveness of the ISMS controls implemented and by a general meeting of the team. The measurement of indicators is performed monthly.

The Top Management / Top Management Representative, together with the support of the Information Security Manager and the Security Committee is responsible for reviewing the utility of the metrics and indicators generated, as well as its modification, deletion or addition of new indicators.

The Information Security Manager is responsible for the measurement of effectiveness of controls implemented through the generation of indicators and metrics established.

The Information Security Manager, Security Committee and the staff in general must provide all information input data required for the generation of metrics and defined indicators.

1.2. Definitions and Abbreviations

Security Committee: Information Security Management System work team.

Metric: variable to which is assigned a value as the result of a measurement.

Security Indicator:

- Metric is extending through interpretation criteria.
- It is a measurement that provides an estimate or assessment of certain attributes derived from a model regarding identified information needs.

2. Reference documents

Documents associated or linked are listed below:

- ISO/IEC 27001 standard, 9.1
- ISMS-001 Policy, Information Security

3. Description

3.1. Effectiveness Measurement Compliance Meetings

The Security Committee will conduct periodic meetings for the purpose of monitoring the effectiveness of implemented controls and ISMS in general. During the same meeting, the committee will track indicators, incidents and other activities carried out for the ISMS, allowing the team to have a view of the effectiveness of controls.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 400

The topics are in the Security Committee Meeting Spreadsheet, while the results are set out in a document that is styled for this purpose.

3.2. Objective Measurement Process

The Information Security Management System effectiveness should be measured to ensure that the controls are properly treating unacceptable risk

For this purposes Metrics and indicators are defined. They are associated with each of the controls, or groups of selected controls, and more generally to the control objectives.

The measurement process will be useful to:

- Evaluate the effectiveness of the implementation of controls.
- Evaluate the effectiveness of implemented controls.
- Evaluate the effectiveness of the ISMS and the improvement achieved.
- Provide a report on the security level for reviews by Top management, security audits and more broadly to facilitate improvements in security.
- View and communicate the value of security to Stefanini.
- Serve as input to the analysis and treatment of risk.

3.3. Metrics and Indicators

The metrics and indicators should be established considering the information to be obtained. In this sense the metrics and indicators established under:

- Security requirement or business requirement to be covered,
- Objectives of controls that have been selected or etc.

These metrics and indicators are documented on the Strategic Objectives ISMS Spreadsheet.

3.4. Lifecycle

Once metrics have been formalized and a frequency schedule developed, the input data will be reviewed and validated.

3.5. Indicators Review

The metrics and indicators should be reviewed and analyzed annually during the Top Management Review. This analysis should include the usefulness of the metrics and indicators. The analysis should also review changes that have emerged in the environment, requirements, control objectives and controls implemented.

4. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Control for record protection	Retention time
Security Committee Meeting Spreadsheet	ISMS Portal	Top Management Representative or someone	Only Top Management Representative or	2 years

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 401

		designated by him	someone designated by him is authorized to edit data	
Strategic Objectives ISMS Spreadsheet	ISMS Portal	Top Management Representative or someone designated by him	Only Top Management Representative or someone designated by him is authorized to edit data	2 years
ISMS Committee Meetings Minutes	ISMS Portal	Top Management Representative or someone designated by him	Only Top Management Representative or someone designated by him is authorized to edit data	2 years

5. Document management

The owner of this document is the Top Management Representative who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

- Results of the objectives
- Audits results

A current version of this document is available to all staff and under version control on the corporate document control system.

6. Appendices

6.1. Metrics

- Measurement – External Press Notifications
  - Base Measure: Number of Incidents reported by external press organizations.
  - Decision Criteria:
    - Zero incidents reported in the press – No action is required.
    - Greater than zero – Intervention is required with an analysis of cause.
- Measurement – ISMS-Trained Personnel
  - Base Measure: [Number of employees with a core responsibility in the ISMS (Security, ICT, IT, Application team) who have completed ISMS training] / [Total number of employees with a core responsibility in the ISMS who should have completed it]

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 402

- Decision Criteria:
  - 0-60% - Intervention is required, analysis must be conducted to understand reasons for non-compliance.
  - 60-90% - Indicator should be watched closely to prevent slippage
  - 90% - No action is required.

- Measurement – Information Security Training
  - Base Measure: [Number of employees who have completed security awareness training] / [Total number of employees who should have completed security awareness training]
  - Decision Criteria:
    - 0-60% - Intervention is required, analysis must be conducted to understand reasons for non-compliance.
    - 60-85% - Indicator should be watched closely to prevent slippage
    - 85% - No action is required.
- Measurement – Security Incident Resolution
  - Base Measure: [Number of Security Incidents within the month resolved within 21 days] / [Number of Security Incidents within the month]
  - Decision Criteria:
    - 0-75% - Intervention is required, analysis must be conducted to understand reasons for non-compliance.
    - 75-90% - Indicator should be watched closely to prevent slippage
    - 90% - No action is required.
- Measurement - Corrective Action Implementation
  - Base Measure:
    - Number of Corrective Actions planned to date
    - Number of Corrective Actions completed by due date
    - Number of Corrective actions not implemented by due date
  - Derived Measure:
    a) [Corrective actions not implemented to date] / [Corrective Actions planned to date]
    b) [Corrective Action not implemented without reason] / [Corrective Actions planned to date]
    c) Compare status with previous status.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 403

- Decision Criteria:
  - In order to conclude the achievement of the objective and no action, the ratios of indicator a) and b) should fall respectively between 0.4 and 0.0 and between 0.2 and 0.0, and Trend of indicator c) should have been declining for the last 2 reporting periods. The indicator c) should be presented in comparison with previous indicators so that the trend in corrective action implementation can be examined.

- Measurement – Frequency of Management Review
  - Base Measure:
    - Number of Management Review meetings planned to date
    - Number of managers scheduled to attend
    - Number of meetings actually held
    - Number of managers actually attending
  - Derived Measure
    a) [Number of meetings actually held] / [Management Review meetings planned to date]
    b) Compute mean and standard deviation of participation rates to review meetings
  - Decision Criteria:
    - Resulting ratio of indicator a) should fall between 0.7 and 1.1 to conclude the achievement of the control objective and no action. Even if it fails, it should be still over 0.5 to conclude the least achievement. With regard to indicator b), Computed confidence limits based on the standard deviation indicate the likelihood that an actual result close to the average participation rate will be achieved. Very wide confidence limits suggest a potentially large departure and the need for contingency planning to deal with this outcome.

- Added Metric – Frequency of ISMS Committee Review
  - Base Measure:
    - Committee Review meetings planned to date
    - Number of people scheduled to attend
    - Number of meetings actually held
    - Number of people actually attending
  - Derived Measure:
    a) [Number of meetings actually held] / [committee meetings planned to date]
    b) Compute mean and standard deviation of participation rates to committee meetings

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 404

- Decision Criteria:
  - Resulting ratio of indicator a) should fall between 0.7 and 1.1 to conclude the achievement of the control objective and no action. Even if it fails, it should be still over 0.5 to conclude the least achievement. With regard to indicator b), Computed confidence limits based on the standard deviation indicate the likelihood that an actual result close to the average participation rate will be achieved. Very wide confidence limits suggest a potentially large departure and the need for contingency planning to deal with this outcome.

- Measurement – Protection Against Malicious Code
  - Base Measure: [Number of security Incidents caused by malicious code] / [Number of detected and blocked attacks caused by malicious software]
  - Decision Criteria:
    - Trend of detected attacks that were not blocked over multiple reporting periods. Compare ratio with the previous percentage. Resulting trend should be downward or constant.
- Measurement – Security in Third Party Agreements
  - Base Measure: Average percent of relevant security requirements addressed in third party agreements.
  - Decision Criteria:
    - Greater than 90% – No action is required.
    - Less than 90% – Intervention is required with an analysis of cause.
- Measurement - IT Services Availability
  - Base Measure: Monthly availability uptime for IT services
  - Decision Criteria:
    - 0 – 95.0% - Intervention is required, analysis must be conducted to understand reasons for non-compliance.
    - 95.0 - 99.9% - Indicator should be watched closely to prevent slippage
    - 99.9% - No action is required.

7. Change history

Date	Version	Created by	Description of change
22-JAN-2014	1.0	Rodrigo Ricci	Document creation
22-SEP-2016	2.0	Matthew Engler	Added appendix of additional metrics.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 405

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 406

BUSINESS CONTINUITY MANAGEMENT POLICY

Information Security Management System



Code:	ISMS-031
Version:	5.0
Date of version:	28-AUG-2020
Created by:	Licsileth Palma
Approved by:	Washington Souza
Confidentiality level:	Internal Use

Table of contents

1. PURPOSE, SCOPE AND USERS 3
1.1. DEFINITIONS AND ABBREVIATIONS 3
1.2. RESPONSIBILITIES 3
2. REFERENCE DOCUMENTS 4
3. DESCRIPTION 4
3.1. INCLUSION OF INFORMATION SECURITY IN THE BUSINESS CONTINUITY MANAGEMENT PROCESS 4
3.2. ASSESSMENT OF BUSINESS CONTINUITY AND RISK 4
3.3. DEVELOPING AND IMPLEMENTING CONTINUITY PLANS 5
3.4. STRUCTURE PLANNING FOR BUSINESS CONTINUITY 5
3.5. TESTING, MAINTENANCE AND REVALUATION OF BUSINESS CONTINUITY ACTIONS 5
4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 5
5. DOCUMENT MANAGEMENT 5
6. APPENDICES 5
7. CHANGE HISTORY 6

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 408

1. Purpose, scope and users

This policy is established to counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disaster of information systems, and ensure timely restoration.

In this case, Stefanini implements a business continuity management process, in order to minimize the impact and recovery from loss of information assets in the organization (which may be the result of, for example, natural disasters, accidents, equipment failures, and deliberate actions) to an acceptable level through a combination of preventive and recovery controls.

Users of this document are the Information Security Manager and the Information Security Committee.

1.1. Definitions and Abbreviations

Significant Event (IT) - A Significant Event (IT) is an outage to a system or service delivered to the end-users (customers / employees) where the entire system or service is unavailable. It may also include a situation where performance has degraded to such a point that, for all practical purposes, the service or system is unavailable for end users. This event results in an interruption of Services for an actual or expected period of more than 4 hours, but less than 24 hours.

Disaster Level Event - A Disaster Level Event is an outage to several systems or services with such significant impact that a large portion of the end-user (customers / employees) population is prevented from normal job functions through several customer / enterprise systems for a period of time. This event results in an interruption of Services for an actual or expected period of more than 24 hours. This may include:

- Any incident that results in physical danger, either by fire, smoke or flood.
- Any incident that indirectly affects business functions such as:
    - Problems accessing the Data Center
    - Building Evacuation by bomb threat
    - Closure of business
    - Fire in another area of the building or in adjacent buildings
    - Natural disasters at regional level: winds, floods, etc.
- Any external incident that could potentially cause a business disruption, such as lack of energy supplies, communications problems, etc.
- Hardware Failures
- Software Failures
- Building Structural Failures
- Sabotage

1.2. Responsibilities

Top Management shall:

- Assign appropriate responsibilities within the business continuity process

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 409

- Allocate resources required for successful implementation of the process
- Disseminate the importance of business continuity plan for all staff
- Identify events that can cause interruptions to business processes

The Department Manager shall:

- Test the arrangements at planned intervals, with the exception of certain tests which may be conducted as required by building or city code (e.g. fire drill)
- Disseminate the plan to all persons who have any responsibility for it
- Keep the Continuity Plan, reviewing it at planned intervals

The Information Security Manager shall:

- Ensure the maintenance of the business continuity plan
- Plan, design and supervise the execution of the business continuity plan annual testing.
- Ensure that the tests are valid and effective.

2. Reference documents

The associated documents are listed below:

- ISO/IEC 27001 standard, A.6.1.3, A.17.1.1, A.17.1.2, A.17.1.3, A.17.2.1
- ISMS-001 Policy, Information Security
- Change Management Process
- Business Continuity Plan
- Evacuation Plan (each facility)

3. Description

3.1. Inclusion of information security in the business continuity management process

Stefanini develops and maintains the business continuity management throughout the organization, which addresses the information security requirements required for business continuity within the scope of the ISMS.

3.2. Assessment of business continuity and risk

The Organization identifies events that can cause interruptions to business processes, along with the probability and impact of such interruptions and their consequences for information security.

In turn, the organization should determine the level of business impact for each of the areas covered by the scope of the ISMS. The Business Impact will be reviewed every two years.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 410

3.3. Developing and implementing continuity plans

Stefanini develops and implements plan to maintain or restore operations and ensure availability of information at the required level and time scales after the interruption or failure of critical business processes.

3.4. Structure planning for business continuity

Stefanini maintains a single structure of business continuity plans to ensure that all plans are consistent and consistently addressing the information security requirements, and to identify priorities for testing and maintenance.

Note: In Stefanini Colombia, the document to use is **Business Continuity Plan IN-MM-02**

3.5. Testing, maintenance and revaluation of business continuity actions

Stefanini performs periodic testing, at least once a year, of its business continuity plans to ensure they are current, effective and valid to fulfill the requirements.

The maintenance plan must be permanent and integrated with the Change Management Process.

4. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Control for record protection	Retention time
Business Continuity Plan - Result	ISMS Portal	Information Security Committee or someone designated by him	Only the Information Security Committee or someone designated by him is authorized to edit data	2 years

5. Document management

The owner of this document is the Information Security Manager who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

- Lesson-learned results

A current version of this document is available to all staff and under version control on the corporate document control system.

6. Appendices

- Not applicable

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 411

7. Change history

Date	Version	Created by	Description of change
22-JAN-2014	1.0	Rodrigo Ricci	Document creation
26-AGO-2014	2.0	Elaine Vanessa	Removed "ISMS-026" and added Evacuation Plan of each facility" under reference documents
04-SEP-2015	3.0	Matthew Engler	Re-assigned some responsibilities to Department Manager; Updated review period of impacts to every 2 years.
26-SEP-2019	4.0	Paulo de Tarso	Updated to clarify the responsibility in register the results in order to ensure that they are valid and effective.
28-AUG-2020	5.0	Licsileth Palma	Included for Colombia **Business Continuity Plan IN-MM-02**

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 412

stefanini
POWERING YOUR BUSINESS

MANAGEMENT OF NON-COMPLIANCE PROCEDURE

Information Security Management System



Code:	ISMS-031
Version:	1.0
Date of version:	22-JAN-2014
Created by:	Rodrigo Ricci
Approved by:	Washington Souza
Confidentiality level:	Internal Use

Table of contents

1. PURPOSE, SCOPE AND USERS 3

2. REFERENCE DOCUMENTS 3

3. DESCRIPTION 3

3.1. DEFINITIONS 3

3.2. COMPLAINTS 3

4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 3

5. DOCUMENT MANAGEMENT 3

6. APPENDICES 4

7. CHANGE HISTORY 4

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 414

1. Purpose, scope and users

The purpose of this document is to describe the controls and responsibilities for treating the systems, services or processes that are non-compliant which originate in the Stefanini Environment.

2. Reference Documents

- ISO/IEC 27001 standard, 10.1
- ISMS-019 Procedure, Risks Identification and Assessment
- Risks, Assets and Classification
- Control Processes (ISO20000)

3. Description

3.1. Definitions

NC: Non-Compliance.

Systems, Services or Processes non-compliance: product, process or service that isn't compliant with the specified requirements.

Correction: When the responsible party takes an action to eliminate items where non-compliance has been detected. One correction can be realized along with corrective action.

Responsible Party: The manager, director, vice president or chief officer (CXO) who is responsible for an area of delivery or a department.

3.2. Complaints

The methods to use the Relationship Management Process are described in the "Relationship Processes" of ISO 20000.

4. Managing records kept on the basis of this document

- Not applicable

5. Document management

The owner of this document is the Information Security Manager, who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

- Changes in the criteria to management the incidents or complaints

A current version of this document is available to all staff and under version control on the corporate document control system.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 415

6. Appendices

- Not applicable

7. Change history

Date	Version	Created by	Description of change
22-JAN-2014	1.0	Rodrigo Ricci	Document creation

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 416

CONFIGURATION MANAGEMENT PROCEDURE

Information Security Management System



Code:	ISMS-033
Version:	2.0
Date of version:	25-AUG-2020
Created by:	Licsileth Palma
Approved by:	Washington Souza
Confidentiality level:	Internal Use

Table of contents

1. PURPOSE, SCOPE AND USERS 3
2. REFERENCE DOCUMENTS 3
3. DESCRIPTION 3
4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 3
5. DOCUMENT MANAGEMENT 3
6. APPENDICES 4
7. CHANGE HISTORY 4

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 418

1. Purpose, scope and users

The purpose of this document is to describe the procedure to administrate versions of components developed by the Software Department. It contains daily and periodic activities to be followed by the Software Department members, and activities that support the Development Maintenance Process.

This document is applied to the entire Information Security Management System (ISMS) and to the Software Department configuration management.

This policy applies to Stefanini Employees, sub-contractors, consultants, business associates, and other workers at Stefanini, including all personnel affiliated with third parties and subsidiaries on the Stefanini infrastructure (collectively "User(s)").

2. Reference Documents

- ISO/IEC 27001 standard, A.9.4.5, A.12.1.2
- ISMS-019 Procedure, Risks Identification and Assessment
- Risks, Assets and Classification
- Control Processes -> Configuration Management Process (ISO20000)

3. Description

The methods to use Configuration Management are described in the "Control Processes" of ISO20000.

Note: For Stefanini Colombia, the procedure to be used is Gestión de la Configuración PC-PP-07, supported by Policy Named Versioned Git Proyectos ADS IN-DD-26 and Gestión de la Configuración IN-PP-06.

4. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Control for record protection	Retention time
Configuration Items Plan	Portal of Operation	Configuration Manager	Only Top Management Representative and Internal Auditors have access	2 years after closure

5. Document management

The owner of this document is the Information Security Manager, who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

- Changes in the Control Version Tool

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 419

A current version of this document is available to all staff and under version control on the corporate document control system.

6. Appendices

- Not applicable.

7. Change history

Date	Version	Created by	Description of change
22-JAN-2014	1.0	Rodrigo Ricci	Document creation
25-AUG-2020	2.0	Licsileth Palma	The use of the Gestión de la Configuración PC-PP-07 procedure is included for Colombia, supported by the Policy Named Versioned Git Proyectos ADS IN-DD-26 and Gestión de la Configuración IN-PP-06.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 420

SECURE DATA DISPOSAL PROCEDURE

Information Security Management System



Code:	ISMS-035
Version:	3.0
Date of version:	25-AUG-2020
Created by:	Licsileth Palma
Approved by:	Washington Souza
Confidentiality level:	Internal Use

Table of contents

1. PURPOSE, SCOPE AND USERS 3
2. REFERENCE DOCUMENTS 3
3. DESCRIPTION 3
4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 6
5. DOCUMENT MANAGEMENT 6
6. APPENDICES 6
7. CHANGE HISTORY 6
APPENDIX A 7
APPENDIX B (COLOMBIA) 11

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 422

1. Purpose, scope and users

The purpose of this document is to detail the media sanitization process.

The users of this document are the analysts responsible for the media sanitization process in notebooks, workstations, servers and SAN for Northern Hemisphere infrastructure.

2. Reference documents

- ISO/IEC 27001 standard, A.11.2.7
- ISMS-001 Policy, Information Security
- ISMS-037 Policy, Media Sanitization and Disposal

3. Description

Media will be disposed using the following methods. The analyst will determine which path needs to be followed, sanitized or physical destroyed. It is preferable that both steps be completed for material which will be disposed of:

Media Type	Sanitize	Physical Destruction
Networking Devices		
Routers	Perform a full manufacturer's reset to reset the router back to its factory default settings. *** Please contact the manufacturer for proper sanitization procedure.*	▪ Pulverize ▪ Shred
Equipment		
Copy Machines	Perform a full manufacturer's reset to reset the router back to its factory default settings. *** Please contact the manufacturer for proper sanitization procedure.*	▪ Pulverize ▪ Shred
Fax Machines	Perform a full manufacturer's reset to reset the router back to its factory default settings. *** Please contact the manufacturer for proper sanitization procedure.*	▪ Pulverize ▪ Shred
Magnetic Media		
Hard Drives	1. Sanitize using Secure Erase or similar software. The Secure Erase software can be download from the University of California, San Diego (UCSD) CMRR site.	▪ Pulverize ▪ Shred ▪ Drill through Platter

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 423

	For Stefanini Colombia, the hard drive is first formatted and then disinfected using the CBL Data Shredder DoD 5220.22-M Method software or similar software. The CBL Data Shredder DoD Method 5220.22-M software can be downloaded from the site: https://www.cbldatarecovery.com/data-shredder/ 2. Or Sanitize hard disk drives by either purging the hard disk drive in an NSA/CSS-approved automatic degausser or by disassembling the hard disk drive and purging the enclosed platters with an NSA/CSS-approved degaussing wand.** **Degaussing any current generation hard disk will render the drive permanently unusable.	
USB Removable Media (Pen Drives, Thumb Drives, Flash Drives, Memory Sticks) with Hard Drives	1. Sanitize using Secure Erase or similar software. The Secure Erase software can be download from the University of California, San Diego (UCSD) CMRR site. 2. Or Sanitize hard disk drives by either purging the hard disk drive in an NSA/CSS-approved automatic degausser or by disassembling the hard disk drive and purging the enclosed platters with an NSA/CSS-approved degaussing wand.** **Degaussing any current generation hard disk will render the drive permanently unusable.	▪ Pulverize ▪ Shred ▪ Drill through Platter

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 424

Magnetic Tapes		
Reel and Cassette Format Magnetic Tapes	Sanitize magnetic tapes by either re-recording (overwriting) or degaussing. Clearing a magnetic tape by re-recording (overwriting) may be impractical for most applications since the process occupies the tape transport for excessive time periods. Sanitize by Overwriting: Overwriting should be performed on a system similar to the one that originally recorded the data. For example, overwrite previously recorded classified or sensitive VHS format video signals on a comparable VHS format recorder. All portions of the magnetic tape should be overwritten one time with known nonsensitive signals. Sanitize by Degaussing: Purge the magnetic tape in any degausser that can purge the signal enough to prohibit playback of the previous known signal. Purging by degaussing can be accomplished easier by using an NSA/CSSapproved degausser for the magnetic tape.	▪ Shred
Optical Disk		
CDs / DVDs	See Physical Destruction	Destroy in order of recommendations: ▪ Removing the Information bearing layers of DVD media using a commercial optical disk grinding device. ▪ Incinerate optical disk media (reduce to ash) using a licensed facility. ▪ Use optical disk media shredders or disintegrator devices to reduce to particles that have a nominal edge dimensions of five millimeters (5 mm) and surface area of twenty-

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 425

		five square millimeters (25 mm2). ** ** This is a current acceptable particle size. Any future disk media shredders obtained should reduce DVD to surface area of .25mm.
Virtual Disk		
SAN Storage VDISK	Delete VDISK instance with the SAN Infrastructure.	N/A

4. Managing records kept on the basis of this document

- Not applicable

5. Document management

The owner of this document is the Infrastructure and Support Department that must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

- Process resulting in negative impact to the business
- Identification of failure at following the procedure.
- Number of incidents related to the procedure.

A current version of this document is available to all staff and under version control on the corporate document control system.

6. Appendices

- Appendix A
- Appendix B: Colombia

7. Change history

Date	Version	Created by	Description of change
02-MAY-2014	1.0	Matthew Engler	Document creation
04-SEP-2015	2.0	Matthew Engler	Combined ISMS-035NH and ISMS-035SH into a single document.
25-AUG-2020	3.0	Licsileth Palma	Description update and appendix B added for CBL Data Shredder software

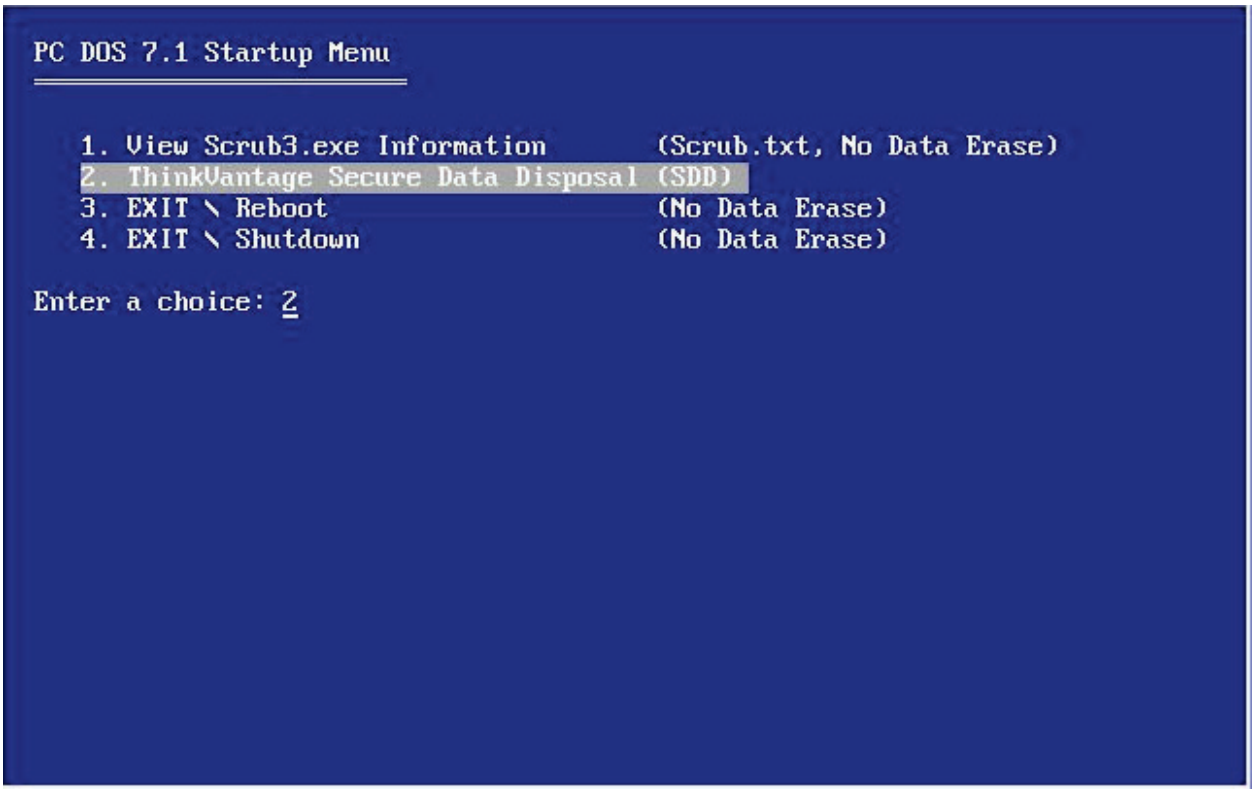
Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 426

Appendix A

The WIPE process (HD - hard Disk formatting) using the Secure Data Disposal tool. The users of this process are the analysts responsible for the image deploy process in notebooks and workstations in Brazil.

The necessary resource for the performance of this activity is: Secure Data Disposal tool CD.

Restart the station to be formatted using the Secure Data Diposal tool CD. As soon as the machine is on, a blue screen will be displayed with 4 options to be chosen, as shown below:



Choose the option 2 (two) ThinkVantage Secure Data Disposal (SDD). After that, the screen below will be displayed, requesting the choice of the HDs to be formatted. Type the corresponding number or choose "All" for all.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 427

```
       What DISK would you like to overwrite?
Note: Your system may not have all disk listed

 A = ALL           = All Disks in System

 1 = First         = First disk

 2 = Second        = Second disk

 3 = Third         = Third Disk

 4 = Fourth        = Fourth Disk

 5 = Fifth         = Fifth Disk

 6 = Sixth         = Sixth Disk

 7 = Seventh       = Seventh Disk

 8 = Eighth        = Eighth Disk

 X = eXit          = EXIT (No SDD, Exit SDD.bat)

Select Disk to Scrub [A,1,2,3,4,5,6,7,8,X]?_
```

Next screen will request the quantity of times the HD should be re-recorded. Chose the option “D” of DOD.

```
          ThinkVantage Secure Data Disposal (SDD)
          =======================================

 What LEVEL of Disposal would you like to invoke?

 L = LIMITED = Overwrite MBR, first 100 sectors and last 2 sectors on each
               partition on ALL drives overwritten with 0x0000 pattern

 M = MEDIUM  = All sectors on ALL drives overwritten 1 time with 0x0000 pattern

 H = HIGH    = All sectors on ALL drives are overwritten 4 times with the
               following patterns (in this order): random pattern, bit-wise
               complement of that random pattern, a different random pattern,
               and a 0x0000 pattern

 D = DoD     = All sectors on ALL drives are overwritten 7 times with the
               following patterns (in this order): random pattern, bit-wise
               complement of that random pattern (3 times, each with a
               different random pattern), and a 0x0000 pattern

 X = eXit    = EXIT (No Overwrites, Exit SDD.bat)

Select Level [L,M,H,D,X]?_
```

Chose the option “Y” for yes in order to leave the partition signature as default.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 428

```
 H = HIGH     = All sectors on ALL drives are overwritten 4 times with the
                following patterns (in this order): random pattern, bit-wise
                complement of that random pattern, a different random pattern,
                and a 0x0000 pattern

 D = DoD      = All sectors on ALL drives are overwritten 7 times with the
                following patterns (in this order): random pattern, bit-wise
                complement of that random pattern (3 times, each with a
                different random pattern), and a 0x0000 pattern

 X = eXit     = EXIT (No Overwrites, Exit SDD.bat)

Select Level [L,M,H,D,X]?D

           ThinkVantage Secure Data Disposal (SDD)
           =======================================

 Y = Yes        = (Default) write scrub signature partition on Disk\s

 N = No         = Scrub disk without creating signature partition

 X = eXit       = EXIT (No Overwrites, Exit SDD.bat)

Write Scrub signature on Disk? [Y,N,X]?
```

Next step will start the HD formatting.

```
Select Level [L,M,H,D,X]?D

           ThinkVantage Secure Data Disposal (SDD)
           =======================================

 Y = Yes        = (Default) write scrub signature partition on Disk\s

 N = No         = Scrub disk without creating signature partition

 X = eXit       = EXIT (No Overwrites, Exit SDD.bat)

Write Scrub signature on Disk? [Y,N,X]?Y

ThinkVantage Secure Data Disposal Utility v3.0
Licensed Materials - Property of Lenovo
(c) Copyright LENOVO 2005  All Rights Reserved.

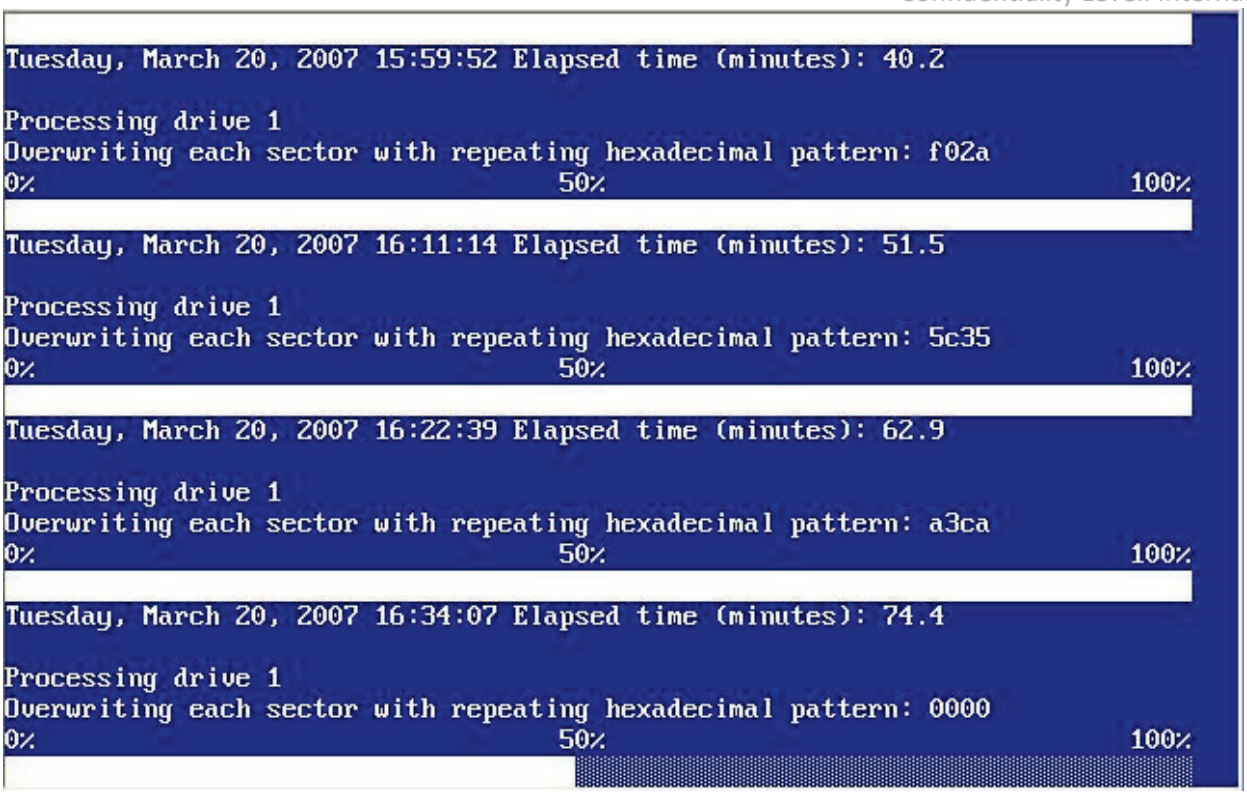
RDMCM003I Execution started at: Tuesday, March 20, 2007 15:19:43

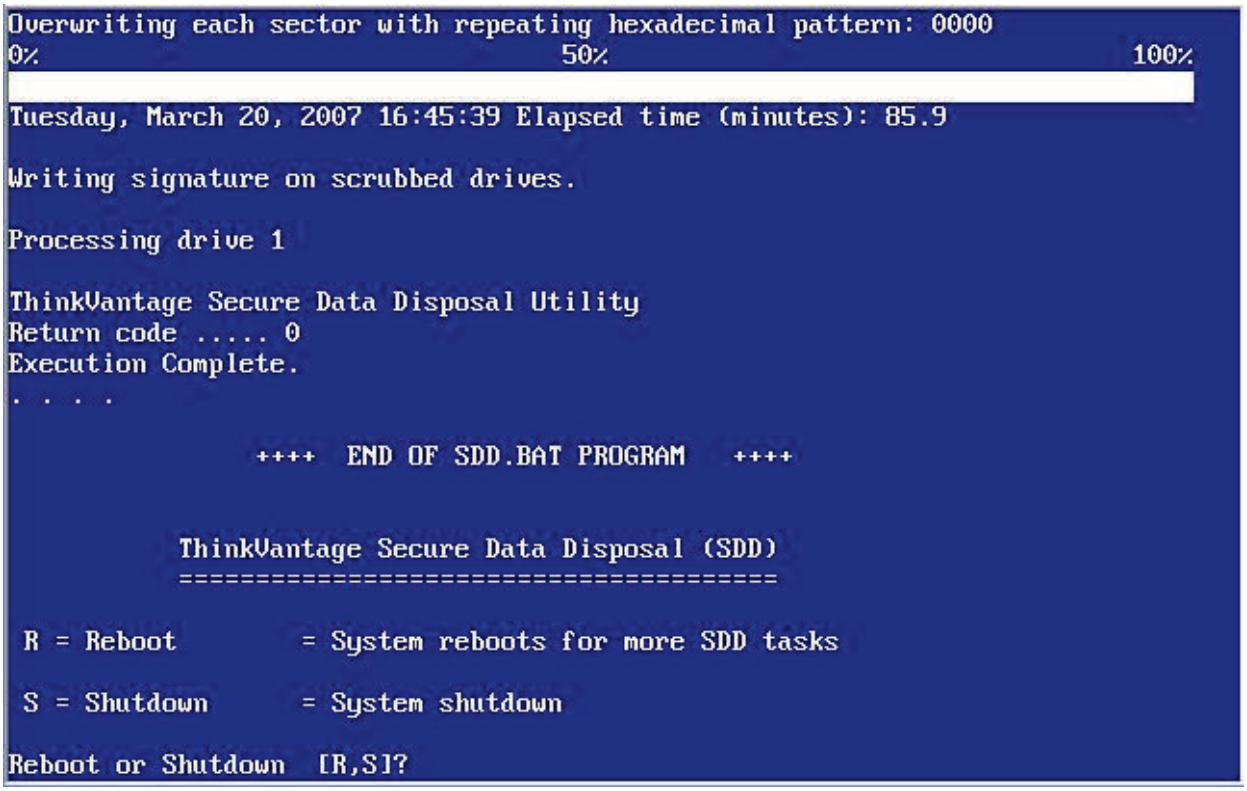
Number of (physical or RAID logical) drives found: 1

Processing drive 1
Overwriting each sector with repeating hexadecimal pattern: 6106
0%                                50%                                100%
```

Note, by checking the screens below, that it is necessary to wait all HD recordings to be finished for the process to be over.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 429





After the process is finished, chose Reboot (option “R”) or Shutdown (option “S”).

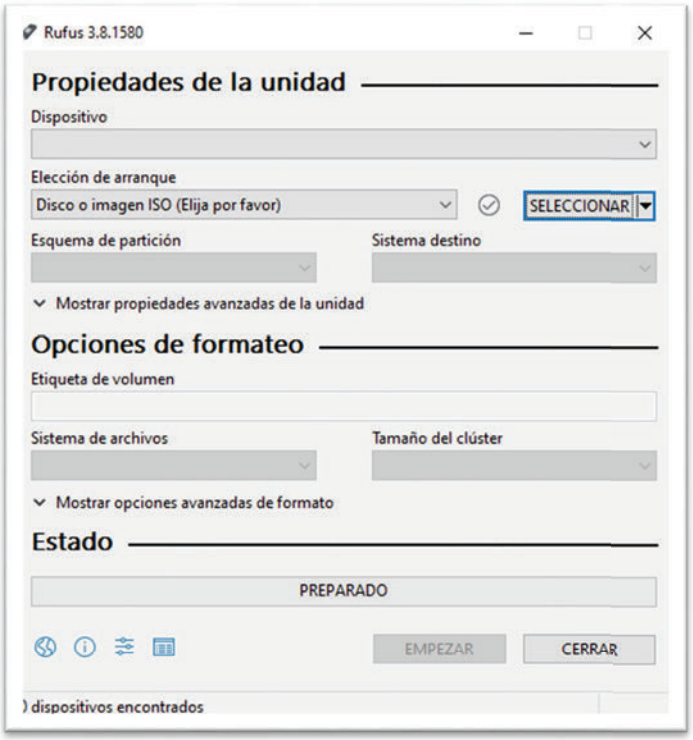
Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 430

Appendix B (Colombia)

The WIPE (HD - Hard Drive Format) process using the Secure Data Delete tool. The users of this process are the analysts of the service desk, responsible for the process of implementing images in laptops and workstations in Colombia.

The necessary resource for the performance of this activity is: CD of the CBL Data Shredder tool DoD Method 5220.22-M.

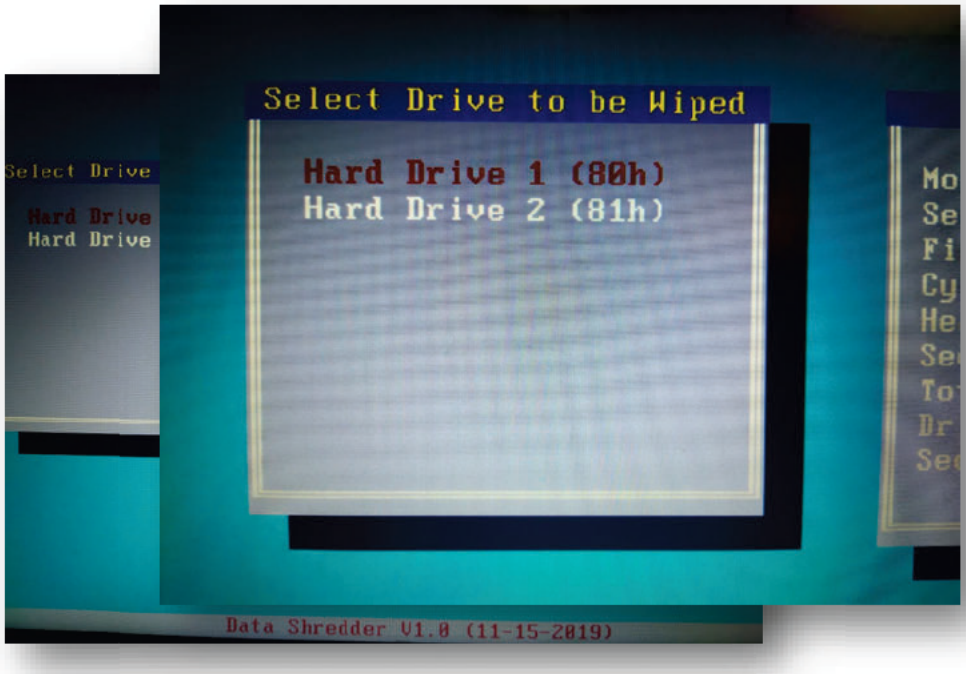
1. Download CBL DATA SHREDDER from the following link https://www.cbldatarecovery.com/data-shredder/ (it will leave you a file in iso format that we will use later)
2. Download the RUFUS program to boot onto a USB pendrive from the following link https://rufus.ie/ (install once downloaded)
3. 3. Once the RUFUS program is installed, it will show you an interface like this



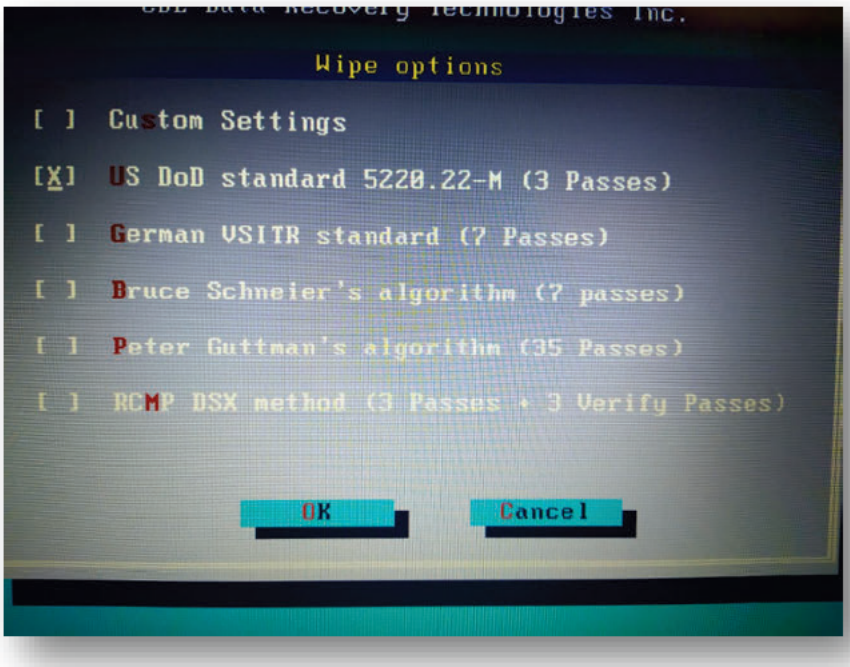
4. Select the USB stick to which you want to load the CBL DATA SHREDDER secure erasure program (in the device area)
5. Select in (Boot choice) the iso that you previously downloaded from CBL DATA SHREDDER
6. Once you carry out these steps, click on start.
7. When it is finished you eject the memory.
8. You insert the memory to the equipment (off) that you want to format.
9. When you turn on the computer, press F9 (for DELL) to execute the boot command and select the USB to execute the CBL DATA SHREDDER program
   Note: for other computers, check the boot execution on its official page
10. Once you have selected the USB, you will see an image like the following

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 431

11. Press enter and the following interface will appear (all the information on your hard drive appears)

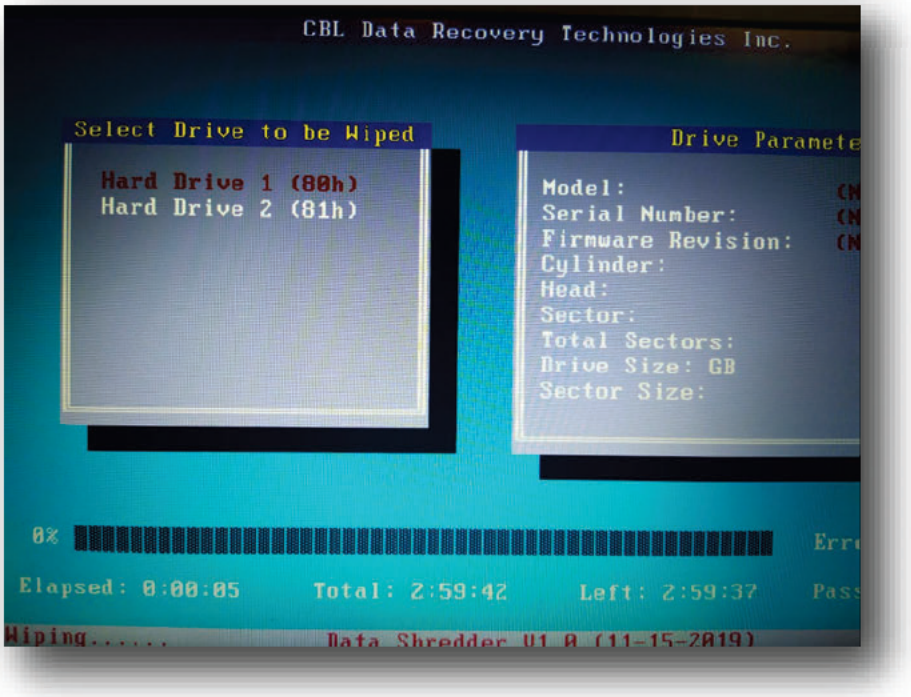


12. Select the partition on which you want to run one of the CBL DATA SHREDDER processes
13. Once you select the partition, the different erasure modes offered by CBL DATA SHREDDER will appear (select one of them)



Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 432

14. When you have selected one of the methods, its execution will begin and depending on the method, the waiting time will be.



15. Once this process is finished, an image like the one below will appear indicating that the process has finished, and your hard drive has been safely formatted with no way to recover the information.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 433

stefanini
POWERING YOUR BUSINESS

FACILITY ACCESS CONTROL AND MONITORING

Information Security Management System



Code:	ISMS-036NH
Version:	6.0
Date of version:	04-SEP-2015
Created by:	Matthew Engler
Approved by:	Stéphane Olmanst
Confidentiality level:	Internal Use

Table of contents

1. PURPOSE, SCOPE AND USERS 3
1.1. RESPONSIBILITIES 3
2. REFERENCE DOCUMENTS 3
3. DESCRIPTION 4
3.1. DEFINITIONS 4
3.2. FACILITY ACCESS GENERAL OVERVIEW 4
3.3. CONTROL OF SERVICE PROVIDERS AND WORKING AFTER-HOURS PERSONNEL 5
3.4. VISITOR ACCESS GENERAL OVERVIEW 6
3.5. VISITOR NETWORK ACCESS 7
3.6. ADDITIONAL VISITOR INFORMATION 7
3.7. RECORDS REVISION AND REPORTS GENERATION 8
3.7.1. Daily reviews and after-hours reports 8
3.7.2. Audit 8
4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 8
5. DOCUMENT MANAGEMENT 9
6. APPENDICES 9
7. CHANGE HISTORY 9

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 435

1. Purpose, scope and users

The purpose of this document is to describe the steps to control people and resources´ entrance and exit to Stefanini´s buildings, as well as monitor and generates reports based on the records of the security cameras and entrance and exit records.

It specifies how people should be identified within Stefanini´s perimeter and how the processing resources that enter and leave the company should be verified and registered.

This policy applies to Stefanini Employees, sub-contractors, consultants, business associates, and other workers at Stefanini, including all personnel affiliated with third parties and subsidiaries on the Stefanini infrastructure (collectively "User(s)"). This policy, in general, refers to any site owned by or leased by Stefanini, including co-location datacenters. Please refer to individual policy statements for applicability to a site based upon size.

1.1. Responsibilities

The Information Security Manager is responsible for verifying compliance with this policy.

The front desk staff / vendor relationship staff is responsible for:

- Controlling the entrance of people into controlled areas.
- Registering visitors according to what was established in this policy.
- Notifying the responsible person when a visitor arrives, if required.

All personnel involved with such business are responsible for:

- Reporting any unauthorized access to the Information Security Manager, HR Management or immediate supervisor.
- Keeping track of the visitors during all visitations.
- The employee responsible for a visitor must register the access according to this document.
- Checking the exit of all received visitors, and in the absence of the receptionist, registering the leaving of the visitor on the appropriate spreadsheet.

The Information Security Manager or designated personnel is responsible for:

- Monitoring the installed video cameras.
- Reviewing the after-hours cameras recordings when necessary.

2. Reference documents

Documents associated or linked to this one are listed below:

- ISO/IEC 27001 standard, 9.1, A.9.1.1, A.9.1.2
- ISMS-001 Policy, Information Security
- ISMS-022, Policy, Clear Desk and Clear Screen

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 436

- ISMS-031 Policy, Business Continuity Management
- ISMS-045 Policy, Physical and environmental security
- Incident Management Process (ISO 20000)

3. Description

3.1. Definitions

Secured Areas: The secure areas are defined by *ISMS-045 Policy, Physical and environmental security.* Access to secure areas is restricted to authorized personnel.

Small Site: Any facility leased or owned by Stefanini where the total number of users who normally work in the facility is less than 25. This does not apply to co-location/data centers.

Medium Site: Any facility leased or owned by Stefanini where the total number of users who normally work in the facility is between 25 and 100. This does not apply to co-location/data centers.

Large Site: Any facility leased or owned by Stefanini where the total number of users who normally work in the facility is greater than 100.

Co-Location: Any facility leased by Stefanini for the purposes of co-locating data and infrastructure. This is normally considered a datacenter. This would not apply to an ASP hosted arrangement.

3.2. Facility Access General Overview

Facilities access controls are maintained through an automated identification process that includes on-boarding procedures to add and remove people from databases or lists that control access to Stefanini facilities. These procedures are auditable. Further, records will be kept as to whom is allowed to access each area of the facility and logs will be maintained that will identify everyone who has entered and exited each secured area. Offices unable to utilize automated access control systems must be authorized and documented by the Information Security Manager with separate procedures defined.

- Applies to Medium Site, Large Site, Co-Location

Internally secured areas of Stefanini facilities must have a separate process for granting access.

- Applies to Small Site, Medium Site, Large Site, Co-Location

Any secured access doors must remain closed and never be propped open without proper approval from Local Stefanini Facilities Departments or the Information Security Manager.

- Applies to Small Site, Medium Site, Large Site, Co-Location

Stefanini Users must not allow anyone through secured doors without a valid Stefanini issued Photo ID and electronic key card where used. Those without these items must be directed to enter through the facility's visitor entrance for further verification. If the person attempting access into the facilities is a visitor, please also see Visitor Access section.

- Applies to Medium Site, Large Site, Co-Location

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 437

Where cipher locks are used for Secured Rooms, combinations must be changed at a minimum twice per year. New combinations will be communicated to needed parties through secured communication and also provided to the Information Security Manager for secured storage.

- Applies to Small Site, Medium Site, Large Site, Co-Location

All Stefanini Users are required to visibly wear a Stefanini issued Photo ID Badge. Anyone found on Stefanini premises without a Photo ID must be reported to management immediately.

- Applies to Medium Site, Large Site, Co-Location

Any Stefanini Facility with offices and or windows located on the ground level must ensure window coverings are drawn and lights turned off at the end of each day to prevent visibility into the building after hours and ultimately prevent theft.

- Applies to Small Site, Medium Site, Large Site, Co-Location

All network drops located within Stefanini facilities that are abandoned (e.g., empty cubes, offices) will be disconnected from the central patch panel or disabled at the switch to prevent unauthorized connection to the Stefanini network. Requests for activating and deactivating Ethernet drops must be made through the Stefanini Service Desk.

- Applies to Small Site, Medium Site, Large Site, Co-Location

Only Stefanini owned, authorized, and approved computers will be connected to the Stefanini internal network. If visitor access is required, please see the Visitor Access section.

- Applies to Small Site, Medium Site, Large Site, Co-Location

If Stefanini Equipment and or property has been damaged, lost, stolen, borrowed or is otherwise unavailable for normal business activities, the primary User must promptly inform their manager, local facilities department or the Information Security Manager to file a claim and provide additional details for investigation purposes.

- Applies to Small Site, Medium Site, Large Site, Co-Location

Stefanini shall retain records in the most economical and practical method and location, and shall destroy or relocate them to more economical storage when appropriate. When not being used by authorized Users, or when not clearly visible in an area where authorized Users are working, all hardcopy confidential or restricted information must be locked in file cabinets, desks, safes, or other furniture. Please refer to *ISMS-022, Policy, Clear Desk and Clear Screen*.

- Applies to Small Site, Medium Site, Large Site, Co-Location

3.3. Control of service providers and working after-hours personnel

Authorization must be requested to the Information Security Manager or through the Infrastructure and Support Management, every time an employee finds it necessary to:

- Enter the facilities out of working hours;
- Request the service of a provider out of working hours.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 438

Request and authorizations must be documented via either:

- Email
- Request within Ticketing System

If a Request has been authorized, notification must be sent to the appropriate Security personnel (if available):

- For visitors - name, Identification Number, represented company and the name of Stefanini´s responsible person.
- For employees - name

This is done in order to coordinate the access authorizations with the Security Company personnel who guard the building, if applicable.

All access is registered on the "After-hours Registration Form", having the following information filled in:

- Name, identification number, represented company, date and time of entry and exit of the building.

3.4. Visitor Access General Overview

There are two categories of visitors to a Stefanini facility:

- Stefanini Personnel Visitor – A Stefanini Employee / Contingent Worker may visit another facility where they are not normally stationed. These personnel are subject to Stefanini Information Security Management System policies and controls, including bound by confidentiality statements.
- 3rd Party Visitor – All other visitors fall under this category

3rd Party Visitors are required to enter and exit through the local facility's visitor entrance only. This process ensures all 3rd party visitors are registered and logged in and out.

- Applies to Small Site, Medium Site, Large Site, Co-Location

When either a Stefanini Personnel Visitor or 3rd Party Visitor enters a Stefanini Facility, they will be required to provide positive picture identification to the receptionist. For Stefanini Personnel Visitor this may be their Stefanini photo ID badge. All 3rd Party Visitors must also read the posted non-disclosure statement and sign a visitor register acknowledging their acceptance to the non-disclosure statement.

- Applies to Medium Site, Large Site

Once a 3rd Party Visitor has signed in, they will be issued a Stefanini Visitor ID Badge. Where available, this badge will be self-expiring and include the visitor's photo. Visitor Badges must be worn at all times. Employees are instructed to immediately report anyone not wearing a Visitor or Employee badge. Stefanini Personnel Visitors may be issues a visitor ID badge as well, or may use their Stefanini-issued photo ID badge.

- Applies to Medium Site, Large Site, Co-Location

A Stefanini User (Sponsor) is responsible for the whereabouts of their 3rd Party Visitors at all times while on Stefanini property and must ensure that their 3rd Party Visitors sign out before leaving the premises.

- Applies to Small Site, Medium Site, Large Site, Co-Location

All Visitors requiring access to areas controlled by swipe card access locks will arrange temporary cards with their sponsor. Departments that have swipe card access locks in their area may have a small number of temporary swipe cards available.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 439

- Applies to Medium Site, Large Site, Co-Location

3rd Party Visitors who are at Stefanini for multiple days must follow all procedures associated with this policy (Check-In, visitor badge, etc.) on each day of their visit. Longer term contractors can be sponsored for a photo-ID badge / badge access by a department. This requires approval from local facility management or the Global Information Security Office.

- Applies to Medium Site, Large Site, Co-Location

At the end of the business day, the receptionist (or equivalent) will verify the visitor log for any 3rd Party Visitors that have not yet exited the facility. The receptionist will notify the person responsible for the visitor that they will be required to log the visitor's exit.

- Applies to Medium Site, Large Site

3.5. Visitor Network Access

Guest computers must not be connected to internal network resources and must be physically secured to prevent unauthorized connection to the Stefanini network unless authorized and administered by local ICT Departments in cooperation with the Global Information Security Office. Users will notify ICT via a Stefanini Service Desk Request in advance if they know their guests will require access. In most major offices, wireless access is available for guests on a separate and dedicated segment. Use of guest wireless is subject to the *Wireless Internet Access Service Disclaimer*.

- Applies to Small Site, Medium Site, Large Site, Co-Location

Guests and other non-organizational users may be given access to the Stefanini Network, production ICT networks and/or its resources by an organizational sponsor through the Information Security Team. The Information Security team will review these requests and grant access as needed (e.g. Auditors, Contractors, Vendors). Guest usernames will be assigned only for the duration that access is required and will be revoked when that access is no longer needed. As with all network traffic, their connections will be monitored via internal systems.

- Applies to Small Site, Medium Site, Large Site, Co-Location

If accessing the Stefanini network / production ICT networks, the sponsor will provide the 3rd Party Visitors a copy of *ISMS-10, Policy, Acceptable Use* for review. After credentials are arranged, activities on the network will be subject to the *ISMS-10, Policy, Acceptable Use*. Visitor use of employee credentials is not permitted under any circumstances. The sponsor will be responsible for monitoring the guest user.

- Applies to Small Site, Medium Site, Large Site, Co-Location

3.6. Additional Visitor Information

In the event of an emergency, it is the sponsoring employee's responsibility to ensure that the Visitor remains in the Evacuation assembly point. Safety Coordinators will tally all Visitors using the Visitor Check-In information. Visitors will not leave the property until it is confirmed with the Safety Coordinators that they have successfully evacuated the building.

- Applies to Medium Site, Large Site, Co-Location

All Visitors are not permitted to take photographs inside of Stefanini premises, unless discussed specifically with sponsoring employees. For instance, photographs are sometimes required for documentation purposes.

- Applies to Small Site, Medium Site, Large Site, Co-Location

Dedicated cameras are not permitted onsite. Cell phones and laptops equipped with cameras are permitted, but as previously stated photographs are not permitted without permission.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 440

- Applies to Small Site, Medium Site, Large Site, Co-Location

3.7. Records revision and reports generation

3.7.1. *Daily reviews and after-hours reports*

Should unauthorized access occur, noted through a review of previous camera footage or via some other notification, the Incident will be reported Human Resources Management and registered in the ticketing system.

The Receptionist will deliver the Visitors Access and after-hours spreadsheets quarterly to the Information Security Manager.

3.7.2. *Audit*

A list of users who have access to a Secured Room, including datacenter and co-location facilities, will be audited quarterly. This audit may be conducted by the owner of the room or by the Information Security Manager.

- Applies to Medium Site, Large Site, Co-Location

A list of users who have accessed the Secured Room, including datacenter and co-location facilities, will be audited quarterly. Focus should be placed on any repeated attempt by a user who does not have proper access. This audit may be conducted by the owner of the room or by the Information Security Manager.

- Applies to Medium Site, Large Site, Co-Location

Auditable records, including who has access and who has attempted to access, will be maintained for at least 90 days. Records may be maintained as either printed, "live" or on electronic media (e.g. backup tapes).

- Applies to Medium Site, Large Site, Co-Location

4. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Control for record protection	Retention time
Visitor_Registration Form	Reception and Infrastructure and Support Department or System	Receptionist	Only the Information Security Manager have the right to edit the document	1 year
After-hours Registration Form	Reception and Infrastructure and Support Department or System	Receptionist	Only the Information Security Manager have the right to edit the document	1 year
Access Audit Reports	Information Security Cabinet	Information Security Manager	Only the Information Security Manager have the right to edit the document	3 Years

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 441

5. Document management

The owner of this document is the Information Security Manager, who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

- Number of incidents related to failures on identifying visitors;
- Number of control incidents;
- Number of unauthorized accesses and unreported entries incidents.

A current version of this document is available to all staff and under version control on the corporate document control system.

6. Appendices

- Not Applicable

7. Change history

Date	Version	Created by	Description of change
04-FEB-2003	1.0	Brandon Ruggirello	Document creation
06-FEB-2003	2.0	Brandon Ruggirello	Added the following statement: local site procedures can be found in iDoc
13-FEB-2009	3.0	Brandon Ruggirello	Modified format for readability
01-MAY-2013	4.0	Matthew Engler	Added audit section for Facilities policy and clarification on Visitor Policies.
02-MAY-2014	5.0	Matthew Engler	Modified formatting to new standard; Added section on camera review.
04-SEP-2015	6.0	Matthew Engler	Clarified visitor access depending upon the type of visitor the person is.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 442

stefanini
POWERING YOUR BUSINESS

MEDIA SANITIZATION AND DISPOSAL POLICY

Information Security Management System



Code:	ISMS-037
Version:	1.0
Date of version:	08-APR-2014
Created by:	Matthew Engler
Approved by:	Washington Souza
Confidentiality level:	Internal Use

Table of contents

1. PURPOSE, SCOPE AND USERS 3
1.1. RESPONSIBILITIES 3
2. REFERENCE DOCUMENTS 3
3. DESCRIPTION 3
3.1. MEDIA SANITIZATION AND DISPOSAL 3
3.2. STEFANINI RAMIFICATIONS 4
3.3. DISPOSAL RECORD 4
4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 5
5. DOCUMENT MANAGEMENT 5
6. APPENDICES 5
7. CHANGE HISTORY 5
APPENDIX A 6

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 444

1. Purpose, scope and users

Data often resides on media, which cannot simply be thrown away. Proper disposal of media is both environmentally responsible and often required by law. In addition, hard drives, USB drives, CD-ROMs and other storage media contain various kinds of Stefanini data, some of which is considered confidential or restricted. In order to protect Stefanini's or any customer's data, all storage mediums must be properly erased before being disposed of. However, simply deleting or even formatting data is not considered sufficient. When deleting files or formatting a device, data is marked for deletion, but is still accessible until being overwritten by a new file. Therefore, special tools must be used to securely erase data prior to disposal. The purpose of this document is to ensure that the media that is no longer needed will be safely and permanently cleaned and removed, minimizing the risks of a security breach and restricted or confidential information exposure caused by negligent or improper disposal methods.

This policy covers all media generated and associated with Stefanini´s information system regardless of their form. It also includes the destruction authorization procedures and disposal treatments of such media.

This policy applies to Stefanini Employees, sub-contractors, consultants, business associates, and other workers at Stefanini, including all personnel affiliated with third parties and subsidiaries on the Stefanini infrastructure (collectively "User(s)").

1.1. Responsibilities

Information asset managers and owners are responsible for ensuring the proper handling of resources used and produced by the information assets' users. They should also ensure that the procedures are appropriate and sufficient for the security, storage and destruction of information assets' storage media.

Users ensure the integrity and confidentiality of the information assets' storage media by complying with all policies and procedures of the Information Security Management System related to their disposal.

2. Reference documents

Documents associated or linked to this document are listed below:

- ISO/IEC 27001 standard, A.8.3.1, A.8.3.2, A.8.3.3
- ISMS-001 Policy, Information Security
- ISMS-028 Policy, Information Classification and Handling
- ISMS-031 Policy, Business Continuity Management
- ISMS-035 Procedure, Secure Data Disposal
- Media Disposal Spreadsheet

3. Description

3.1. Media Sanitization and Disposal

- When information assets have reached the end of their useful life they must be sent to the local Information Technology office for proper disposal.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 445

- Users are responsible for the sanitation of non-reusable paper media in their possession, such as documents, contracts, etc, before disposal. This media must be shredded.
- Users are responsible for the sanitation of non-reusable electronic media in their possession, such as USB drives, CDs, etc, before disposal. Similar to shredding paper reports, CDs and other non-rewritable media should either be broken or defaced by scratching before disposal.
- Local IT will have a process and procedure for proper disposal, which may include 3rd party services for handling disposal.
- Information Technology will securely erase all storage mediums in accordance with current industry best practices.
- Equipment which is working, but reached the end of its useful life to Stefanini may be made available for purchase once all data removal is confirmed by the Information Security office.
- Finance and Information Technology will determine an appropriate cost for each item and have a formal process for handling the sale of approved IT items.
- Prior to leaving Stefanini premises, all equipment must be removed from the Information Technology asset system.

Additional media sanitization guidelines can be found in *NIST Special Publication 800-88, Guidelines for Media Sanitization.*

3.2. Stefanini Ramifications

Failure to properly dispose of technology equipment can have several negative ramifications to Stefanini including fines, negative customer perception and costs to notify affected professionals/customers of data loss or inadvertent disclosure.

3.3. Disposal Record

A record of confidential or restricted information technology disposal will be maintained through the Change Management process. The authorization for the disposal must be clearly identified. To determine the classification, see the "*ISMS-028 Policy, Information Classification and Handling*".

Where requested, Stefanini may provide a Certificate of Destruction. Please see Appendix A.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 446

4. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Control for record protection	Retention time
Ticket related to the disposal request	ISMS Portal or Ticket Management System	Infrastructure and Support Department or someone designated by them.	Only Infrastructure and Support Department or someone designated by them is authorized to edit data.	Minimum of 1 year
Certificate of Destruction (when requested)	Legal Department	Legal	Only the processing contact or someone designated by them is authorized to edit data.	Minimum of 3 Years or per Record Retention Policy for "Contracts"

5. Document management

The owner of this document is the Infrastructure and Support Department that must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

- Process resulting in negative impact to the business
- Identification of failure at following the procedure.
- Number of incidents related to the procedure.

A current version of this document is available to all staff and under version control on the corporate document control system.

6. Appendices

- Appendix A – Certificate of Destruction

7. Change history

Date	Version	Created by	Description of change
08-APR-2014	1.0	Matthew Engler	Document creation

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 447

Appendix A

Certificate of Data Destruction for Data Acquired From [Customer and/or Services]

Requestor Organization		**Data Use Agreement**
Requestor Contact Name		**Phone No.**
Requestor Address		
Processing Organization		
Processing Contact Name		**Phone No.**
Processing Address		
Project Name		
Project Manager (if applicable)		
Data Files Destroyed:	**File**	**Method**
Data Files not Destroyed (Exceptions):	**File**	**Reason**

By signing this Certification of Data Destruction, I confirm that the data acquired under <Contract> have been handled as indicated above.

Processing Contact Printed Name	Signature	Date
Project Manager (if applicable) Printed Name	**Signature**	**Date**

<Stefanini Entity Address>

Commented [MDE1]: Information regarding the requesting company, including reference to contract which discusses data use / destruction.

Commented [MDE2]: Information regarding the data processor or the organization which will be destroying the data. Usually Stefanini.

Commented [MDE3]: Data files destroyed and methodology. Files can be a high level description, for example "Data files stored within Project SharePoint"

Commented [MDE4]: Data files that, for a given reason, could not be destroyed..

Commented [MDE5]: Contact from Processing organization who is certifying destruction.

Commented [MDE6]: Project manager, if applicable, certifying destruction.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 448

stefanini
POWERING YOUR BUSINESS

FIREWALL MANAGEMENT POLICY

Information Security Management System



Code:	ISMS-038
Version:	1.0
Date of version:	11-APR-2014
Created by:	Luiz Robson; Matthew Engler
Approved by:	Washington Souza
Confidentiality level:	Internal Use

Table of contents

1. PURPOSE, SCOPE AND USERS 3
1.1. RESPONSIBILITIES 3
1.2. DEFINITIONS AND ABBREVIATIONS 3
2. REFERENCE DOCUMENTS 3
3. DESCRIPTION 3
4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 5
5. DOCUMENT MANAGEMENT 5
6. APPENDICES 5
7. CHANGE HISTORY 5

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 450

1. Purpose, scope and users

The purpose of this policy is to establish guidelines to detect and prevent unauthorized accesses to internal or external networks, such as the Internet. Also it formalizes what is explicitly allowed by the administration regarding the services provided by and for these networks.

It applies to all security equipment implemented at the Internet access points.

This policy applies to Stefanini Employees, sub-contractors, consultants, business associates, and other workers at Stefanini, including all personnel affiliated with third parties and subsidiaries on the Stefanini infrastructure (collectively "User(s)").

1.1. Responsibilities

Management / Department Managers and Information Security are responsible for authorizing any changes to the rules defined in the Firewall.

The Information Security Manager, or a designated person, is responsible for:

- Conducting a review of a selection of the firewall rules yearly to ensure rules are still required and appropriate.
- Monitoring any security events generated by the firewall and properly following up.
- Take the necessary measures to respond to any incidents detected by the firewall

1.2. Definitions and Abbreviations

Firewall: A combination of hardware and software that separates a local area network (LAN) in two or more parts for security purposes. Its basic goal is to ensure that all communications between the network and the Internet will be made in accordance with the security policies of the organization. Moreover, these systems often incorporate elements of privacy, authentication, etc.

2. Reference documents

Documents associated or linked to this one are listed below:

- ISO/IEC 27001 standard, A.12.2.1
- ISMS-001 Policy, Information Security
- ISMS-031 Policy, Business Continuity Management

3. Description

Access to the Stefanini Network Infrastructure will be protected by industry-standard firewalls with adequate secure rule bases installed. Each large site will be configured in a high availability configuration or with a cold standby redundant firewall to ensure network availability.

All information to and from distinct entities to Stefanini will be monitored by the firewall. All information between areas with different levels of security will also be controlled by it.

Stefanini's internal network addresses will remain private. When systems require access to other networks, the private address will be translated to a legal, registered address prior to transmission.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 451

By the use of the firewall, and of people and procedures, the established access guidelines should be implemented.

Access guidelines

The different decisions formally adopted regarding the communication between Stefanini and external networks (Internet and others) should be documented.

The following items should be taken into consideration for maintenance:

- Communication with third parties must, as much as possible, be made through VPNs or dedicated links.
- Any provided service or communication through the Internet must not expose, in any way, the internal network.
- All critical software, especially the security ones, must receive periodic updates.
- Measures must be implemented in order to enable navigation on the Internet to authorized sites and duly authorized persons, without exposing the internal network. Where available, access to the public Internet will be monitored and restricted with Proxy based URL filtering software.

Management Guidelines

Changes to the firewall rules (providing access, allowing ports, VLAN, etc..) must be approved before being implemented in the firewall. Changes will be completed through the Change management system. Relevant approvals must be captured and must include the Information Security Manager, or someone they designate.

Select rules implemented in the Firewall will be reviewed yearly to ensure they are in accordance with the business requirements and appropriate security needs.

Monitoring Guidelines

The Firewall must register every significant event, such as:

- Configuration changes
- Security events
    - External
    - Internal
- Changes on users with access to it
- Navigation carried out by users

These records must display the date, time, a description or code that indicates the event type, and any other possible technical information.

These records must be available to the Information Security Manager, or someone they designate, for review of any potential security risks to Stefanini.

The Information Security Manager, or someone they designate, should analyze the event log monthly. Any security events or items needing further review should be documented, including the date, time, comments and actions needed. The integrity of the firewall event logs must be guaranteed in all cases, prohibiting access to unauthorized persons.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 452

Software Update

Besides the Firewall, all network devices, as well as switches and routers, should be treated in accordance with the approved process.

4. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Control for record protection	Retention time
Firewall Rule Change	ISMS Portal or Ticket Management System	Infrastructure and Support Department or someone designated by him	Only Infrastructure and Support Department or someone designated by him is authorized to edit data	Minimum of 1 year
Security Event Review	ISMS Portal or Ticket Management System	Infrastructure and Support Department or someone designated by him	Only Infrastructure and Support Department or someone designated by him is authorized to edit data	Minimum of 1 year

5. Document management

The owner of this document is the Information Security Manager, who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

- Amount of rules discovered during audits that are no longer required.

A current version of this document is available to all staff and under version control on the corporate document control system.

6. Appendices

- Not applicable

7. Change history

Date	Version	Created by	Description of change
11-APR-2014	1.0	Luiz Robson; Matthew Engler	Document creation

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 453

ANTI-VIRUS / ANTI-MALWARE SOFTWARE POLICY

Information Security Management System



Code:	ISMS-039
Version:	1.0
Date of version:	11-APR-2014
Created by:	Luiz Robson; Matthew Engler
Approved by:	Washington Souza
Confidentiality level:	Internal Use

Table of contents

1. PURPOSE, SCOPE AND USERS 3

1.1. RESPONSIBILITIES 3

1.2. DEFINITIONS AND ABBREVIATIONS 3

2. REFERENCE DOCUMENTS 4

3. DESCRIPTION 4

3.1. GENERAL POLICY 4

3.2. USERS NOTIFICATION AND VIRUS / MALWARE ELIMINATION 5

4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 5

5. DOCUMENT MANAGEMENT 5

6. APPENDICES 5

7. CHANGE HISTORY 6

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 455

1. Purpose, scope and users

The purpose of this document is to describe how to protect Stefanini computing resources against intrusion and malware infection (viruses or malicious software).

This document is applied to all of Stefanini´s computer devices (desktops, notebooks, Servers, PDAs, Black Berry, etc.), which sporadically and / or continuously have access to the internal network and to the entire Information Security Management System (ISMS).

This policy applies to Stefanini Employees, sub-contractors, consultants, business associates, and other workers at Stefanini (collectively “User(s)”).

1.1. Responsibilities

IT Support / Deskside is responsible for:

- Generating the inventory of all Stefanini´s IT assets and checking for anti-virus;
- Installing anti-virus on computers without it;
- Ensuring that the anti-virus is periodically updated and running without end user interaction;
- Verifying the updates before releasing the update package;
- Performing the post implementation review.

The Infrastructure and Support Department is responsible for:

- Monitoring viruses on their computer networks and taking corrective action;
- Monitoring the disclosure of new vulnerabilities to the operating systems in use within the company;
- Ensuring correction of the vulnerabilities in order to prevent insertion of new viruses;
- Setting the updates frequency, depending on how critical each system is;
- Ensuring that the established rules are being followed.

1.2. Definitions and Abbreviations

Malicious code (malware) is software specifically designed to perform harmful actions and malicious activities on a computer. Some of the different ways in which malicious code can infect or compromise a computer are:

- Exploitation of vulnerabilities in installed programs;
- Infected removable media like pen-drives;
- Access to malicious Web pages using vulnerable browsers;
- Direct action of attackers that, after hacking the computer, insert files containing malicious code;
- Implementation of previously infected files through email messages attachments, removable media and web pages or directly from other computers (due to the sharing of resources).

Once installed, the malicious code may have access to the data stored in the computer and can perform actions on behalf of users, according to the permissions of each user.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 456

The main reasons that lead an attacker to develop and propagate malicious codes may include the gaining of financial benefits, capturing confidential information and the desire of self-promotion and vandalism. Furthermore, malicious codes are often used as intermediates to allow hits, attacks and the spreading of spam.

2. Reference documents

Documents associated or linked to this one are listed below:

- ISO/IEC 27001 standard, 12.2; A.12.2.1
- ISMS-001 Policy, Information Security
- ISMS-010 Policy, Acceptable use
- ISMS-031 Policy, Business Continuity Management
- Report of Assets without anti-Malware.

3. Description

3.1. General policy

- All Stefanini systems as outlined in the scope must have Stefanini's standard and supported anti-virus / anti-malware software installed.
- The anti-virus / anti-malware software should operate continuously on servers and workstations. It is configured to work in real-time (i.e. whenever a file is accessed).
- The anti-virus/anti-malware software and the virus pattern files must be kept up-to-date through an automated method.
- The anti-virus/anti-malware software should perform a full scan in all Stefanini´s workstations and servers at regular intervals:
    - Workstations (Desktops, Laptops) – Once per week
    - File Servers – Once per week
    - All other servers – Per a defined schedule
- In case of a critical virus / malware infection, the Infrastructure and Support Department may take urgent measures with the permission / supervision of the Information Security Manager, including the suspension of the system to prevent the spread of malware to other systems and / or regions.
- Any activities with the intention to create and/or distribute malicious programs into Stefanini's networks (e.g., viruses, malware, worms, Trojan horses, email bombs) are prohibited in accordance with the *ISMS-010 Policy, Acceptable use*.

E-mail:

- All incoming electronic messages must be scanned for virus and malware. If discovered, the system must quarantine these email messages for further action.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 457

3.2. Users notification and virus / malware elimination

If the anti-virus/anti-malware software detects virus / malware or if a user suspects that there is an infection in the network PCs, the user must immediately notify the Infrastructure and Support Department via the Incident Management process.

Users should not attempt to remove viruses / malware from the system by themselves, unless they reside in a department responsible for doing so. If it is discovered that a virus or malware has infected a server, the Infrastructure and Support Department must notify all affected parties in accordance with legal and contractual requirements.

Once the infection is confirmed, infected PCs and / or servers must be disconnected from the Stefanini network in order to eliminate the virus / malware. Systems will not be re-connected to the network until they are verified as virus-free in cooperation with Information Security.

4. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Control for record protection	Retention time
Report of Assets without anti-virus / anti-malware software installed.	ISMS Portal or Software management Console.	Infrastructure and Support Department or someone designated by it.	Only the Infrastructure and Support Department or someone designated by it is authorized to edit data	1 year or until software is installed.

5. Document management

The owner of this document is the Infrastructure and Support Department that must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

- Number of incidents related to malware;
- Number of machines without the Virus-list update;
- How long it takes for the machines in the environment to be updated.

A current version of this document is available to all staff and under version control on the corporate document control system.

6. Appendices

- Not Applicable

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 458

7. Change history

Date	Version	Created by	Description of change
11-APR-2014	1.0	Luiz Robson; Matthew Engler	Document creation

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 459

stefanini
POWERING YOUR BUSINESS

CAPACITY MANAGEMENT PROCEDURE

Information Security Management System



Code:	ISMS-040
Version:	3.0
Date of version:	26-AUG-2020
Created by:	Licsileth Palma
Approved by:	Washington Souza
Confidentiality level:	Internal Use

Table of contents

1. PURPOSE, SCOPE AND USERS 3
1.1. RESPONSIBILITIES 3
2. REFERENCE DOCUMENTS 3
3. DESCRIPTION 3
3.1. AVAILABLE RESOURCES MONITORING 3
3.2. FUTURE REQUIREMENTS PROJECTIONS 3
3.3. NEW ACQUISITIONS 4
4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 4
5. DOCUMENT MANAGEMENT 4
6. APPENDICES 4
7. CHANGE HISTORY 4
APPENDIX A (BRAZIL) 5
APPENDIX B (COLOMBIA) 8

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 461

1. Purpose, scope and users

This document defines the responsibilities, methodology and processes used by Stefanini to do the monitoring and projection of the necessary resources to guarantee the systems adequate performance.

This policy applies to Stefanini Employees, sub-contractors, consultants, business associates, and other workers at Stefanini (collectively "User(s)") and all resources required for the proper functioning of the systems.

1.1. Responsibilities

The Infrastructure and Support department is responsible for:

- Checking the reports generated by the specific software containing a tracking update related to the Company resources.
- Annually generating a projections and acquisitions report associated to the main resources.
- Requesting applicable emergency purchases due to unexpected situations.
- Ensuring the necessary resources availability for the proper functioning of the systems.

2. Reference documents

- ISO/IEC 27001 standard, A.12.1.3
- ISMS-001 Policy, Information Security
- Capacity Management Spreadsheet

3. Description

3.1. Available resources monitoring

The Infrastructure and Support department must submit a report on the adequacy of the required resources for the proper functioning of the systems. Reports may be produced as necessary, but no less than once per year.

Based on it, along with the Product Department Manager, the system projections and their tracking should be developed, as well as the launching of resources acquisitions or other emergency actions due to unexpected situations.

3.2. Future requirements projections

The Product Department Manager will annually present, along with his annual investment plan, a projection of necessary resources to be incorporated.

The monthly monitoring report conducted on these resources will work as justification for such investment.

It is also necessary to consider the resources required by the new projects to be implemented.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 462

3.3. New acquisitions

For all cases, the operational requirements for new systems must be anticipated and established before its approval and use.

4. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Control for record protection	Retention time
Capacity report	ISMS Portal	Servers Team; Infrastructure and Support Department	Only the Infrastructure and Support Department Representative or someone designated by him is authorized to edit data	1 year

5. Document management

The owner of this document is the Infrastructure and Support Department, that must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

- E.g. number of initiated corrective actions

A current version of this document is available to all staff and under version control on the corporate document control system.

6. Appendices

- Appendix A: Brazil
- Appendix B: Colombia

7. Change history

Date	Version	Created by	Description of change
27-JAN-2014	1.0	Luiz Robson	Document creation
04-SEP-2015	2.0	Matthew Engler	Combined Zabbix instructions in single document.
26-AUG-2020	3.0	Licsileth Palma	Update Latest version Zabbix Colombia (Appendix B)

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 463

Appendix A (Brazil)

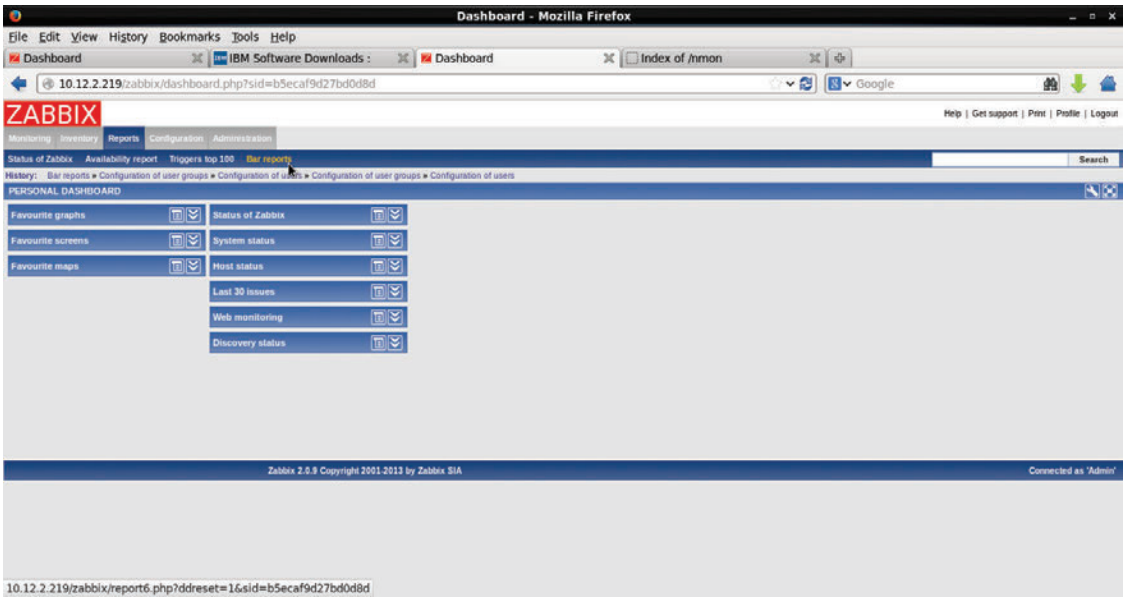
Report Generation through Zabbix (Brazil / LATAM) performed monthly.

For the report generation, the Infrastructure and Support department must:

- Access the ZABBIX tool at the following address: http://10.12.2.19
- Execute login.

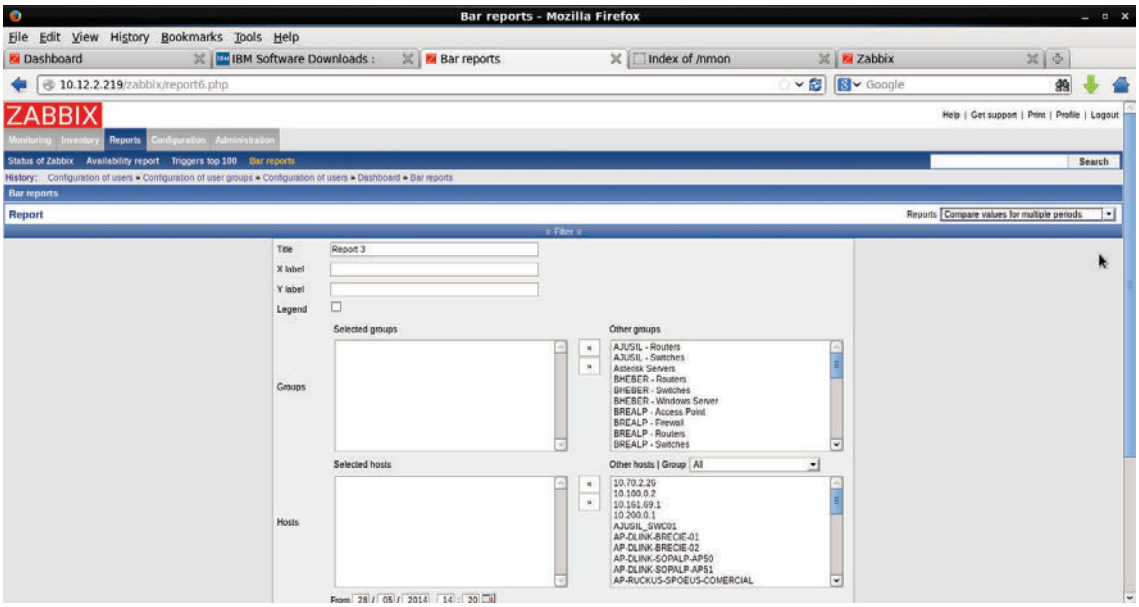


- In the dashboard, choose the “Reports” tab and then, “Bar Reports”

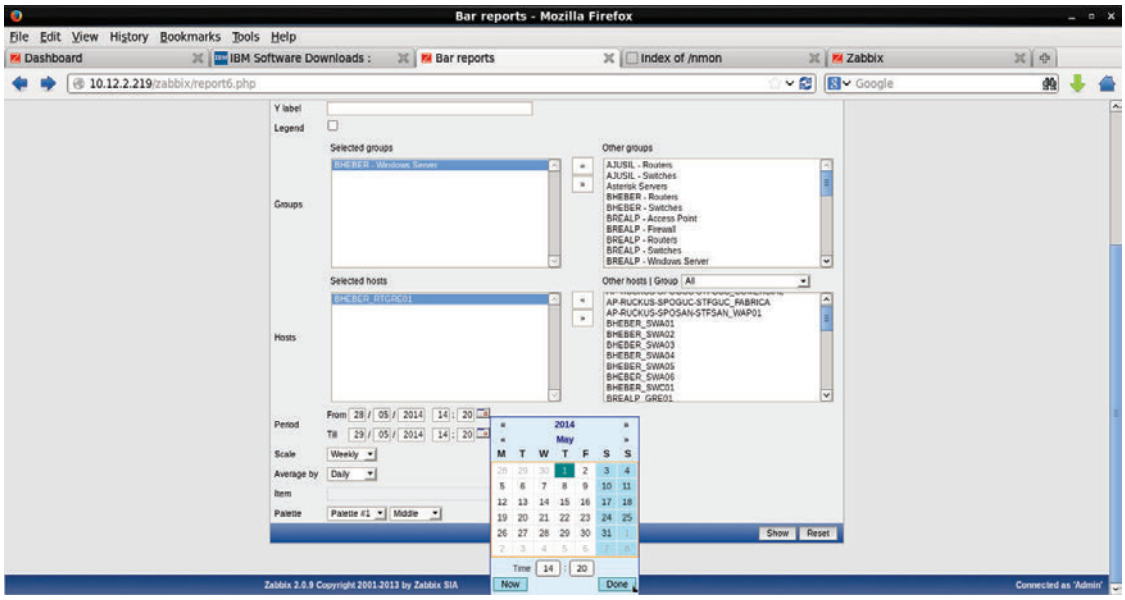


- The system shows the following screen:

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 464

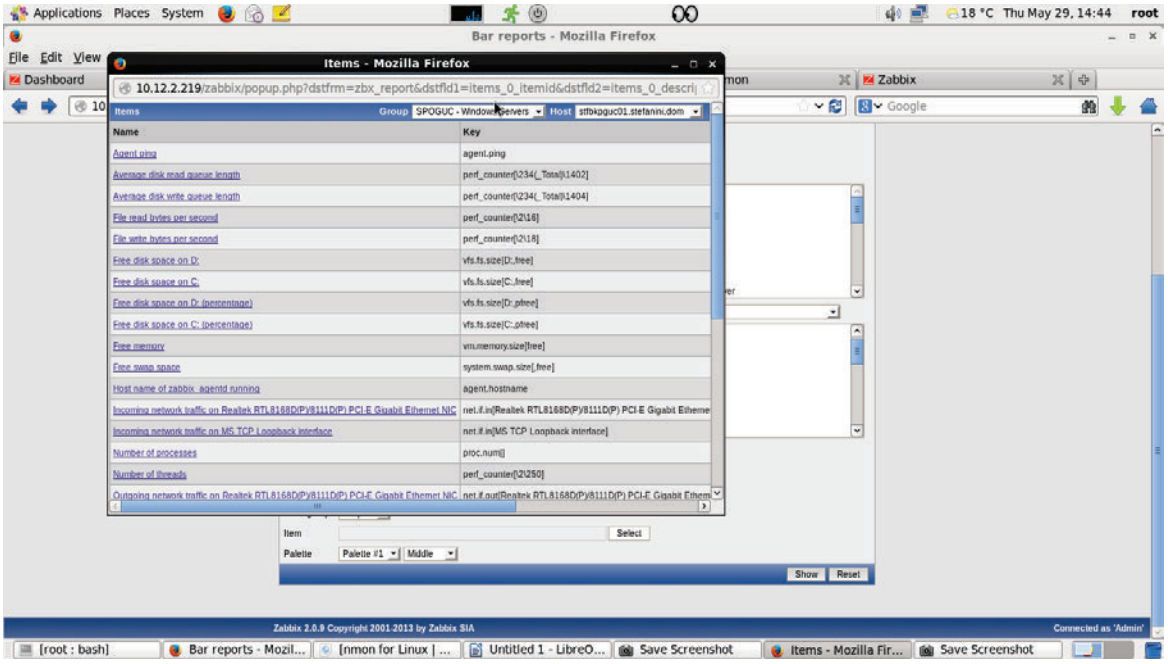


- Add a title to the report
- Select “Compare Values for Multiple Periods” option
- Select the group “Windows Server”
- Select the Host / group
- Select the timeframe

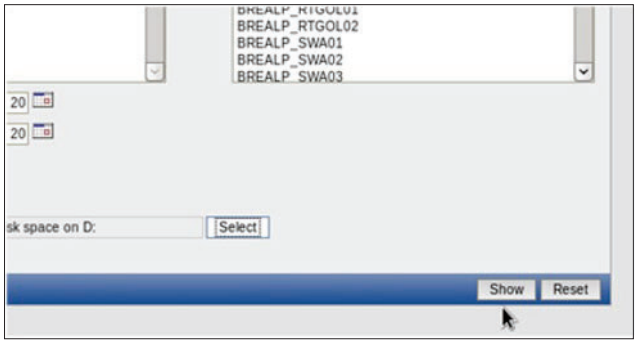


- Select the report items: (Memory usage, Disk space and CPU usage)

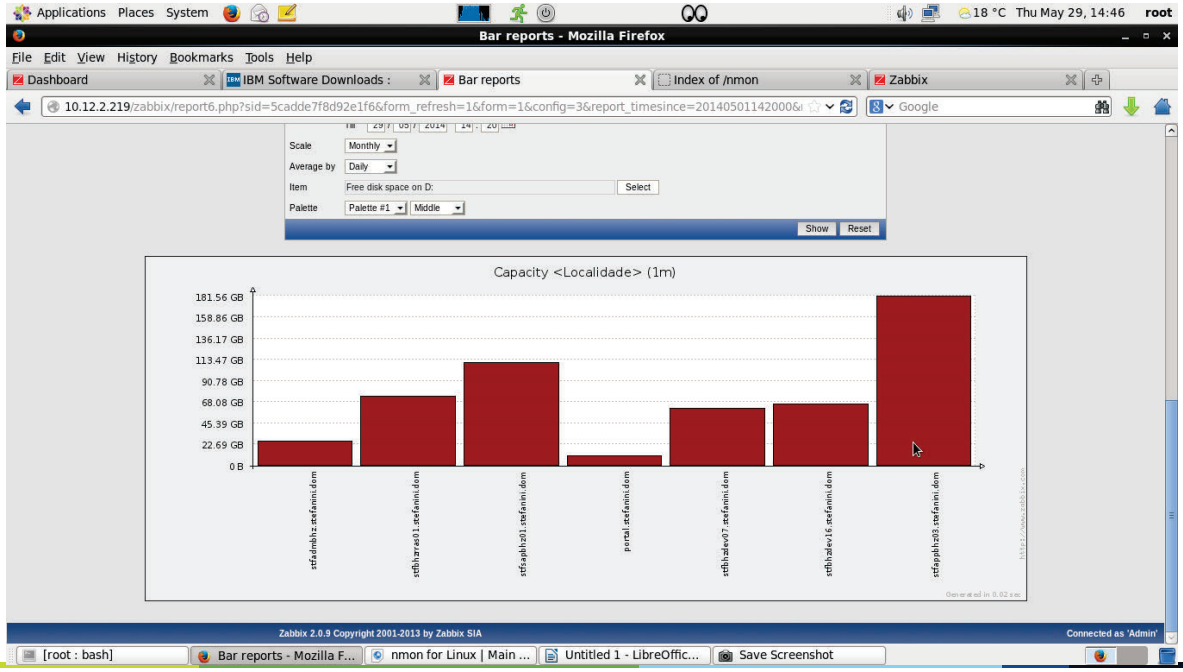
Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 465



- Click the “Show” button:



- A graphic containing the selected information will be displayed.



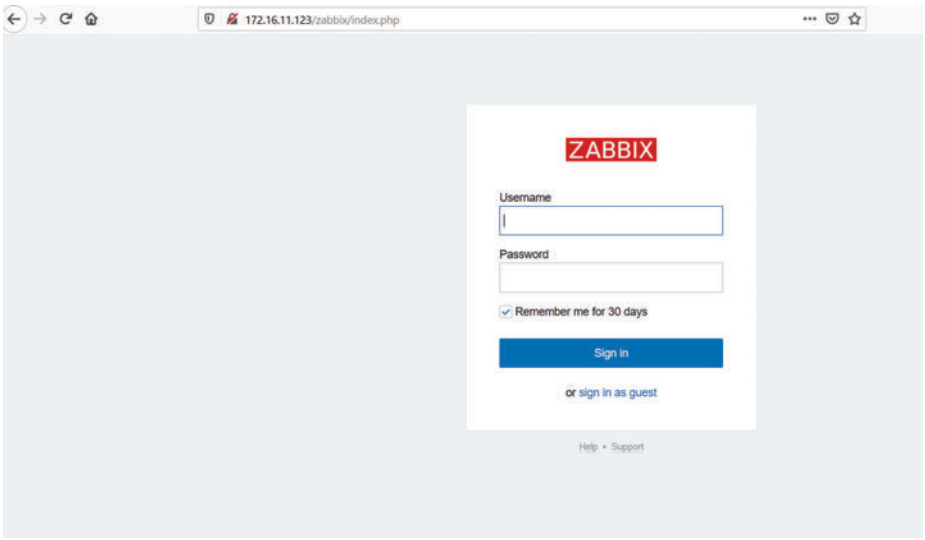
Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 466

- The report must be sent to the Information Security Manager or designated personnel responsible for analyzing the report and taking the relevant actions.

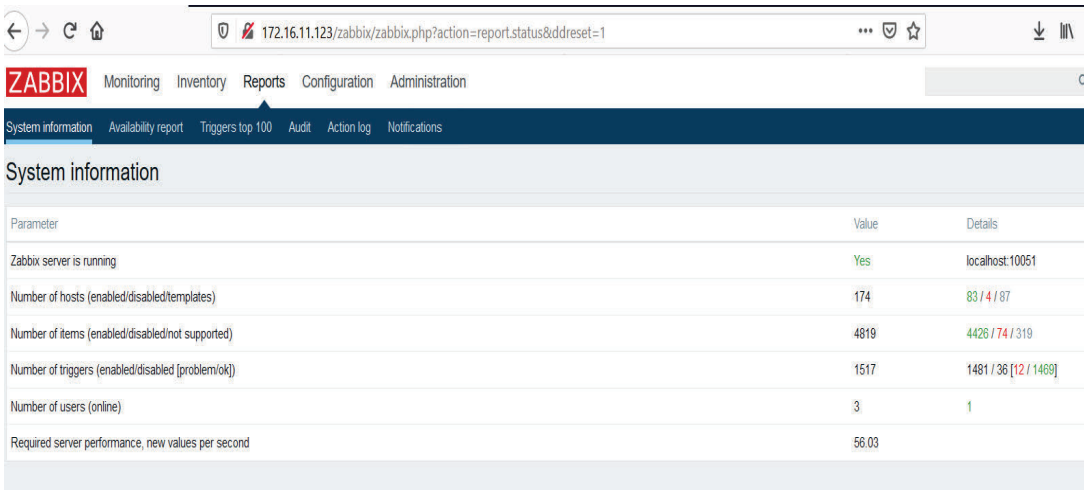
Appendix B (Colombia)

For the generation of reports, the infrastructure and support department must:

- Access the ZABBIX tool at the following address http://172.16.11.123/zabbix
- Login

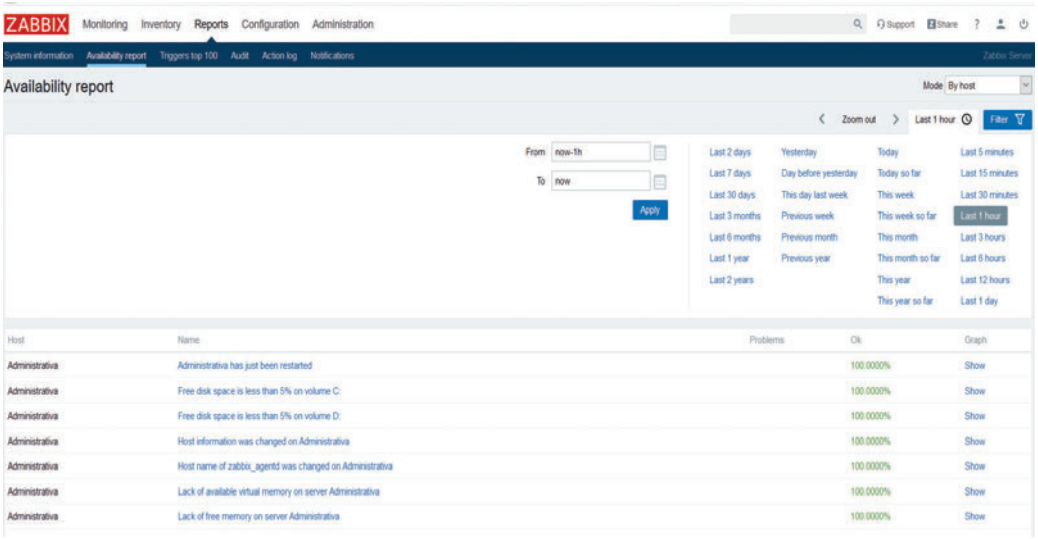


- In the panel, choose the tab "Reports" and then "System Information"

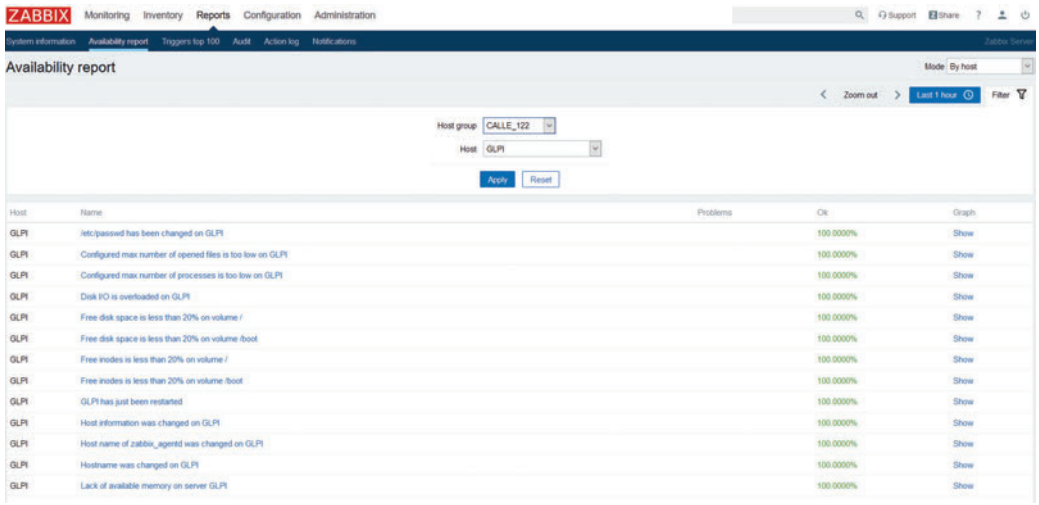


Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 467

- It will show us the information of the Zabbix that is being used at this moment, such as monitored hosts, deactivated hosts and templates used with them in the monitoring part.
- The system will show the following screen, we will press the option “Availability report” in which we will get all the information about the hosts that there are and the different monitors that each team has. We can choose for days, weeks or years.

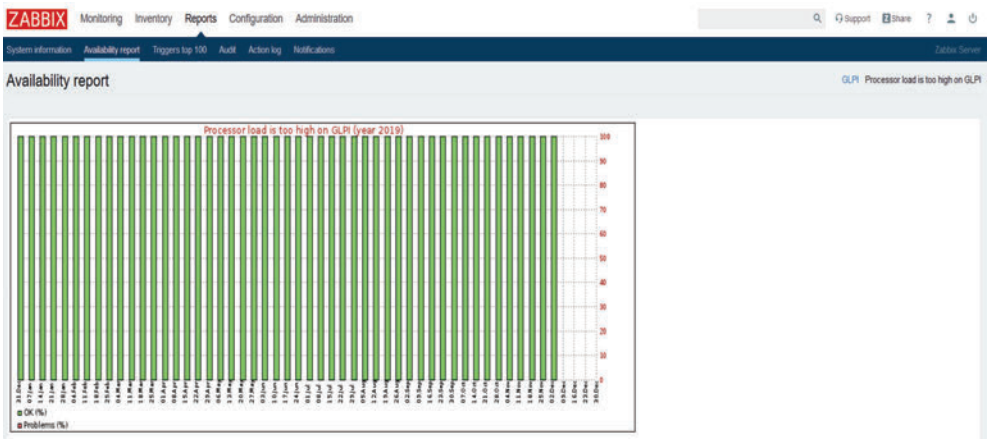


- Select "Filter", we can see the elements that each server, Switch, or Router that is being monitored.



- By pressing “Show” a graphic with the selected information will be displayed.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 468



- The report will be sent with the information cataloged by the security administrator or personnel responsible for examining the report and taking the appropriate measures.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 469

stefanini
POWERING YOUR BUSINESS

COMUNICATIONS AND OPERATIONS SECURITY POLICY

Information Security Management System



Code:	ISMS-041
Version:	3.0
Date of version:	09-AGO-2018
Updated by:	Luiz Robson de Souza
Approved by:	Washington Souza
Confidentiality level:	Internal Use

Table of contents

1. PURPOSE, SCOPE AND USERS 3
2. REFERENCE DOCUMENTS 3
3. DESCRIPTION 3
4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 5
5. DOCUMENT MANAGEMENT 5
6. APPENDICES 6
7. CHANGE HISTORY 6

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 471

1. Purpose, scope and users

The purpose of this policy is to ensure the proper management of Stefanini´s communications and operations.

This policy applies to Stefanini Employees, sub-contractors, consultants, business associates, and other workers at Stefanini, including all personnel affiliated with third parties and subsidiaries on the Stefanini infrastructure (collectively "User(s)").

2. Reference documents

- ISO/IEC 27001 standard, clauses A.12.1.1, A.12.1.2, A.12.1.3, A.12.1.4, A.12.2.1, A.12.3.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.5.1, A.12.6.1, A.12.7.1
- ISMS-001 Policy, Information Security
- ISMS-004 Procedure, Backup system
- ISMS-011 Policy, Change management
- ISMS-012 Procedure, Checking of Log of access and use of systems
- ISMS-033 Procedure, Configuration Management
- ISMS-037 Policy, Media Sanitization and Disposal
- ISMS-039 Policy, Anti-Virus/Anti-Malware Software
- ISMS-040 Procedure, Capacity Management
- ISMS-042 Policy, Removable Storage Media

3. Description

Stefanini is aware of the importance of communications and ICT operations for:

- Meeting the strategic objectives of the organization.
- Meeting the information objectives, ensuring the integrity, availability and confidentiality of all processed information, both internally and of third parties involved.

Therefore, to ensure correct and safe operation of information processing resources, Stefanini should:

Ensure proper and safe operation of the information processing facilities by:

- Documenting operating procedures. These must be kept and made available to all users who need them.
- Formalizing and establishing a procedure to control systems change and information processing facilities properly.
- Segregating duties and areas of responsibility to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.
- Separating resources for development, test and production in order to reduce the risk of unauthorized access or changes to the operating system.
- Formalizing and establishing a catalog of services including availability metrics.

Implement and maintain an appropriate level of information security and service delivery, according to the third party's service delivery contract by:

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 472

- Reasonable assurance that the security controls, service definitions and delivery levels included in the agreements are implemented, operated and maintained by the third party.
- Monitoring and evaluating services and reports provided by third parties.
- Proper management of changes in third party services.

Minimize the risk of system failures

- Monitors and adapts resource usage and projections of future capacity requirements to ensure the required system performance.
- Establishes acceptance criteria for new information systems, upgrades and new versions.
- Performs appropriate system tests during development and prior to acceptance.
- Deploys appropriate system redundancies to meet availability requirements.

Define an anti-malware policy to protect software and information integrity by:

- Implementing controls for the detection, prevention and recovery for protection against malicious code.
- Appropriate user awareness training.

Define a backup policy to maintain the integrity and availability of information and information processing facilities.

- Regular backup of information and software, and tests consistent with the established backup procedures.

Ensure the protection of information in networks and the protection of infrastructure support.

- Manage and control the network correctly in order to protect it against threats, and maintain systems security, including for information in transit.
- Identify security features, service levels and management requirements of all network services.

Prevent unauthorized disclosure, modification, deletion or destruction of information assets, ensuring that business activities are not interrupted. The media should be controlled and physically secured.

- Implement procedures for managing removable media.
- Remove the media securely using formal procedures.
- Establish procedures for the use and storage of information to protect it against misuse or unauthorized disclosure.
- Protect the system documentation from unauthorized access.

Maintain the security of information and software exchanged within the organization and any other entity.

- Implement formal procedures and controls to protect the exchange of information, for the use of any communication feature.
- Establish agreements for the exchange of information and software between the organization and third parties.
- Protect media containing information from unauthorized access, misuse or corruption during transportation beyond the physical boundaries of the organization.
- Adequately protect the information contained in e-mail.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 473

- Establish procedures to protect the information associated with the interconnection of business information systems.

Ensure the integrity and availability of information published electronically through the website. Management of technical vulnerabilities

- Identify probable technical vulnerabilities
- Monitor and manage the vulnerabilities against threats
- Establish a control for each vulnerabilities identified in the risk analysis
- Deploys appropriate system redundancies to meet availability requirements.

Management of environments

- There is an environment for each phase of service/operation, such as development, testing and operational.
- For each network, server, desktop and laptop deployments, the Infrastructure team will define a configuration guide, considering the various customer's requirements;
- The environments are controlled by the Chief of Information Security, who has the control of users and access for each environment.
- For each service, the Service Manager must check and plan the environment, who has Access and what rights.

Detect unauthorized information processing activities.

- Monitor systems log events and information security.
- Administrator and system operators shall be logged with their respective personal password;
- Record and save the audit logs of user activities, exceptions and information security events, for an agreed period to assist in future investigations and access control monitoring.
- Establish procedures to monitor the use of processing information facilities and regularly review the results of the monitoring activities.
- Protect records and information from manipulation and unauthorized access.
- Record the activities of the administrator and system operators.
- Record and analyze detected failures and take appropriate actions.
- Synchronize all the relevant information processing systems clocks with a reliable time source inside the Organization or security domain
- ICT staff who are responsible for the centralized monitoring solution or security scanning must be familiar with the process of reviewing and interpreting security logs, either locally on computers or through a centralized system.
- Scanning for unauthorized wireless networks.
- Scanning the ICT network for unauthorized activity and unauthorized ICT equipment.

4. Managing records kept on the basis of this document

- Not Applicable

5. Document management

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 474

The owner of this document is the Infrastructure and Support Department, who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

- E.g. number of initiated corrective actions
- E.g. number of incomplete corrective actions
- E.g. number of corrective actions taken without having been recorded in a designated form

A current version of this document is available to all staff and under version control on the corporate document control system.

6. Appendices

- Not Applicable

7. Change history

Date	Version	Created by	Description of change
20-JAN-2014	1.0	Luiz Robson	Document creation
04-SEP-2014	2.0	Matthew Engler	Added redundancy requirements
09-AUG-2018	3.0	Luiz Robson	Added reference of devices configurations according customer's requirements

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 475

stefanini
POWERING YOUR BUSINESS

REMOVABLE STORAGE MEDIA POLICY

Information Security Management System



Code:	ISMS-042
Version:	1.0
Date of version:	08-APR-2014
Created by:	Luiz Robson; Matthew Engler
Approved by:	Washington Souza
Confidentiality level:	Internal Use

Table of contents

1. PURPOSE, SCOPE AND USERS 3

1.1. RESPONSIBILITIES 3

1.2. DEFINITIONS AND ABBREVIATIONS 3

2. REFERENCE DOCUMENTS 3

3. DESCRIPTION 3

3.1. REMOVABLE STORAGE MEDIA TREATMENT AND MANAGEMENT: 3

3.2. REMOVABLE STORAGE MEDIA STORAGE AND MAINTENANCE: 4

3.3. REMOVABLE STORAGE MEDIA SECURITY: 4

4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 4

5. DOCUMENT MANAGEMENT 4

6. APPENDICES 4

7. CHANGE HISTORY 5

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 477

1. Purpose, scope and users

The purpose of this policy is to ensure that there are operational and treatment procedures for the management and protection of removable storage media information, associated with Stefanini´s information asset management system. The *ISMS-042 Policy, Removable Storage Media* is defined to minimize the risk of loss or exposure of confidential or restricted information maintained by Stefanini and to reduce the risk of acquiring malware infections on computers operated by Stefanini.

This policy covers the information storage removable media used by Stefanini, like tapes, disks, cassettes, USB devices and paper documents, among others. It also includes the management of removable storage media to prevent loss, damage, theft and unauthorized access to such media, in addition to required procedures for the storage, transportation and maintenance of these repositories.

1.1. Responsibilities

Managers and owners of information assets are responsible for ensuring the proper handling of removable storage media used and produced by the users and information assets under their direct supervision. They must confirm that the procedures are appropriate and sufficient for the safety and maintenance of the removable information storage media.

Users must ensure the integrity and confidentiality of the information assets removable storage media for which they have permissions or access control by complying with all applicable policies and procedures of the Information Security Management System.

Information assets managers and owners must also keep track of the removable storage media accesses inside or outside Stefanini, according to the controls in the *ISMS-027 Policy, Information Transfer*.

1.2. Definitions and Abbreviations

Removable Media: all media that may contain information and is easily transported (diskettes, CDs, USB devices, SD cards, Pen-Driver’s etc...).

2. Reference documents

Documents associated or linked are listed below:

- ISO/IEC 27001 standard, A.8.3.1, A.8.3.3.
- ISMS-001 Policy, Information Security
- ISMS-027 Policy, Information Transfer
- ISMS-037 Policy, Media Sanitization and Disposal
- ISMS-044 Policy, Use of Cryptographic Controls

3. Description

3.1. Removable storage media treatment and management:

Stefanini system users must only use removable media in accordance with assigned job duties or if there is an actual need where data cannot be transferred by using other means. Restricted data may only be stored

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 478

on removable media if your assigned duties require this or when providing information required by other state or federal agencies. Files containing confidential or restricted data stored on removable media must be protected by approved encryption. See also *ISMS-044 Policy, Use of Cryptographic Controls*.

3.2. Removable storage media storage and maintenance:

Removable storage media must be properly stored, regardless of its format, to ensure physical protection and confidentiality control of confidential or restricted data. Please refer to the *ISMS-028 Policy, Information Classification and Handling* for further details.

3.3. Removable storage media security:

Authority to take removable storage media in Stefanini will be established, and usage will be monitored. The access to removable storage media should be handled through given permissions.

Authorization for use of removable media must be formally communicated to the Information Security Manager Department or Top Management / Top Management representative. Unauthorized use of removable media is strictly prohibited.

Stefanini reserves the right to disable the ability to use removable media on any system.

4. Managing records kept on the basis of this document

- Not Applicable

5. Document management

The owner of this document is the Infrastructure and Support Department that must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

- Number of initiated corrective actions
- Number of incomplete corrective actions
- Number of corrective actions taken but not registered in a designated form.

A current version of this document is available to all staff and under version control on the corporate document control system.

6. Appendices

- Not Applicable

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 479

7. Change history

Date	Version	Created by	Description of change
08-APR-2014	1.0	Luiz Robson; Matthew Engler	Document creation

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 480

ACCOUNT AND PASSWORD POLICY

Information Security Management System



Code:	ISMS-043
Version:	2.0
Date of version:	17-JUL-2020
Updated by:	Matthew Engler
Reviewed by:	Elaine Pinheiro
Approved by:	Washington Souza
Confidentiality level:	Internal Use

Table of contents

1. PURPOSE, SCOPE AND USERS 3

2. REFERENCE DOCUMENTS 3

3. DESCRIPTION 3

3.1. ACCESS CONTROL - INTRODUCTION 3
3.2. ACCOUNTS CREATION 3
3.3. MANAGEMENT OF PRIVILEGED ACCOUNTS 5
3.4. MANAGEMENT OF PASSWORDS 6
3.5. PASSWORD USERS OBLIGATIONS 7
3.6. USER PASSWORD MANAGEMENT 8
3.7. REVIEW OF ACCESS RIGHTS 8
3.8. CHANGE OF STATUS OR TERMINATION OF CONTRACT 8
3.9. APPLICATION DEVELOPMENT STANDARDS 9

4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 9

5. DOCUMENT MANAGEMENT 9

6. APPENDICES 9

7. CHANGE HISTORY 9

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 482

1. Purpose, scope and users

The purpose of this document is to define rules for access to various systems, equipment, facilities and information, based on business and security requirements for access. This document is to prescribe rules to ensure secure password management and secure use of passwords.

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Stefanini facility, has access to the Stefanini network, or stores any non-public Stefanini information.

2. Reference documents

- ISO/IEC 27001 standard, A.7.3.1, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6, A.9.3.1, A.9.4.1, A.9.4.2, A.9.4.3, A.18.1.4
- ISMS-001 Policy, Information Security
- ISMS-003 Statement of Applicability
- ISMS-028 Policy, Information Classification and Handling
- ISMS-50 Policy, Non-Expiring Password

3. Description

3.1. Access Control - Introduction

The basic principle is that access to all systems, networks, services and information is forbidden, unless expressly permitted to individual users or groups of users. There should be a user registration procedure for each system and service.

Access to all physical areas in the organization is allowed, except to areas for which privilege must be granted by an authorized person.

This Policy specifies rules for access to systems, services and facilities, while the Information Classification Policy defines rules for access to individual documents and records.

User accounts to computing environments provide access to IT resources and business related activities.
This policy applies to user accounts of all kinds: user accounts, privileged accounts, service accounts (interface between systems), local login accounts, shared accounts, emergency accounts and temporary accounts. The purpose of this policy is to define the requirements for management of these accounts and ensure the appropriate level of protection for these accounts on all computer platforms

All user accounts must comply with certain minimum conditions for its management and use. These conditions differ depending on the use and privilege of these accounts. As a general rule, all accounts must be used and managed so that there is sufficient IT resources and activities for Stefanini´s business protection.

3.2. Accounts creation

Those responsible for business processes, not the IT department, are responsible for determining who needs access, what level of access, what is the purpose of access and what is the duration of the access. It is the responsibility of the "owner" of the business and the definition of these parameters is the responsibility of the

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 483

IT department to ensure that these parameters are followed according to the preference of the "owner" of the business.

Rule 1 - Many applications, database systems employ standard accounts to simplify installation. The name of these standard accounts must be changed (if possible) and default passwords must also be changed.

Rule 2 - The accounts must be assigned by individuals who are responsible for their use. Every user must have an account needing one that is unique among all other accounts and used only by this user.

Additional Note
Security controls should assist in the identification of users to ensure that each user has access to only the necessary assets and resources inside Stefanini.

Rule 3 - The use of shared accounts should be restricted

- A shared account can be used when there are significant limitations to access and when the account has restricted use. Shared accounts may only be used when there is a "business case" documented. This "business case" document must be approved by the "owner" of the business and the regional group of Information Security.

Additional Note
The use of shared accounts is also restricted by the following factors:

- Whenever possible each shared account must be linked to a specific machine so that these accounts can only be used on these machines. These machines should be located in public places.
- Shared accounts may not have remote access (VPN).
- Shared accounts may not be able to generate e-mail messages, unless the email address of the shared account has been approved by management.
- The shared account password should be changed annually or whenever compromised.
- An accurate record of all shared user accounts must be maintained.
- A responsible (owner) identified for each shared account must conduct an annual review to determine whether there is a need to maintain the account.
- Administrator privileges should not be attributed to share accounts.
- Unrestricted access to the Internet is not allowed for shared accounts.

Rule 4 - Use of anonymous accounts must be avoided
Anonymous accounts do not allow you to join the network activity and system with individual users who are responsible for the activity. Anonymous accounts, where required, shall comply with the following criteria:

- Guest ("guest") and other anonymous accounts should be disabled or deleted if they do not have a well-defined purpose.
- If an anonymous "guest" account and is required to run an application, their use should be regularly monitored.
- If there is a "business case" to justify a documented "guest" or anonymous, the policy dictates it should be empowered with a read-only right for non-sensitive data.

Additional Note
Anonymous accounts should be restricted to only allow read access.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 484

Rule 5 - Privileged accounts should only be granted when required. Administrators must have privileged accounts that are limited only to the privileges required.

Rule 6 - Accounts for non-Stefanini users must follow the rules specified in this policy

- Third parties who have access to Stefanini´s computer systems must follow the same rules of account management and strong passwords as Stefanini.
- For each account of a third party, there must be a Stefanini "owner" for this third party account who made the request of the account and accepts responsibility for it.

Rule 7 - Temporary accounts can only be used when appropriate

- Accounts for training, temporary facilities and other conditions of access can be best addressed with temporary accounts that are generic in nature and are not tied to an individual. Temporary accounts are suitable for short-term jobs. The one who requested the temporary account is responsible for its existence and use.

3.3. Management of Privileged accounts

Rule 1 - Use of privileged accounts should be restricted

- Accounts with elevated privileges exist throughout computing platform: The root of UNIX, Sysadmin on an Oracle database, Windows Server Administrator (as well as those who are in the administrators group), service accounts and accounts of superuser applications are examples of accounts that can expose Stefanini to serious security risk. These accounts should be treated with special care, limiting their use and assigning responsibility to individuals whenever possible.
- Accounts with elevated privileges should never be shared outside of the IT support team. The use outside the team for IT support must be approved by management.
- Accounts with elevated privileges and occasional use must be disabled and only activated when needed. After use, these accounts should be disabled again using an emergency procedure change request to process documentation.
- Administrators must, whenever possible, authenticate themselves with their own personal account and then switch to a privileged account, so that all administrator activity can be audited and logged.

Rule 2 - Service accounts can only be used for approved applications

- Service accounts can only be used by applications. Users are not permitted to use a service account to authenticate to applications.
- There is no minimum frequency for changing the password for service accounts, except for accounts system administrator (admin, root, sys, sysadmin, etc.) or internal service accounts of financial systems, payroll or human resources. The service account passwords must be changed whenever compromised.

Additional Note

Service accounts are required to enable communication from one process to another. Service accounts are not user accounts and should not be used as such.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 485

3.4. Management of passwords

Rule 1 - Users must be authenticated before a password can be reset

- All password resets must start with the positive identification of the requesting user. In some cases, local support can forward the request to reset the password for the Service Desk that effectively accomplishes the process. In such cases, the responsibility for positive user identification is with the local support. The Service Desk should be responsible for the positive identification of support when asked. When passwords are reset, the new password should be unique and if possible, the user should automatically be forced to change the password after the first login.
- Positive identification can occur through a call back, leaving the new password in a system user's mailbox, security protocol separately, either personally or through a secondary mechanism of authentication with personal identifiers.

Additional Note
Automated systems for resetting passwords should use multiple checks to positively identify the user.

Rule 2 - Expirations of passwords must follow the approved schedule

- Passwords of servers, user machines, network devices, databases and applications should be changed according to the approved schedule. If possible, the password expiration should be automated. If not, one should ask users to change their passwords based on the following schedule:

Category	Description	Examples	Schedule
User accounts	All accounts not mentioned below	Stefanini Standard (AD) User Windows, Unix, E-Access, RM	90 days
Privileged Accounts	Accounts with elevated privileges and high security risk.	Windows Server Admin, LAN Admin, Unix-root, E- Access Admin	90 days
Services Accounts	Some privileged service accounts administration or application, actively used, from machine to machine and rarely used by humans.	ForefrontService, Application Owning Accounts (PeopleSoft master account) File Transfer (FTP) Accounts	There is no minimum frequency for changing the password for service accounts. The service account passwords must be changed whenever corrupted. Refer to the *ISMS-50 Policy, Non-Expiring Password* for further clarification.
Local Login Accounts	Accounts used when network resources are unavailable.	root or the admin accounts of a server allowing local access	Maximum 30 days
Equipment internal network (user commands and system administrator)	Read-only and elevated privilege of Router / Switch Cisco	Cisco-connect, mstat, mtrace, rlogin, traceroute, where; Cisco-configure, copy, erase, mrinfo, reload, rsh, setup, tunnel	NH : 120 days Brazil/LATAM, 90 days

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 486

Equipment external network (user commands and system administrator)	Read-only and elevated privilege of Router / Switch Cisco	Cisco-connect, mstat, mtrace, rlogin, traceroute, where; Cisco-configure, copy, erase, mrinfo, reload, rsh, setup, tunnel	60 days

Rule 3 - The password complexity should be configured to ensure safety and operability
The password requirements for history, locking and reset must meet the following criteria wherever possible:

Category	Requirement
History	A password may only be repeated after a series of 8 different passwords
Locking	If a user fails to enter the correct password for their account 5 times within 15 minutes, the user account will be disabled for a minimum of 30 minutes.
Reset	A password should expire upon first login, forcing the user to change to a new password.

Additional Note

When a system or application does not have any options for the above settings, manual controls should be used.

3.5. Password users obligations

Users must apply good security practices when selecting and using passwords:

- Passwords must not be disclosed to other people, including management and system administrators
- Passwords must not be written down, unless a secure method has been approved by the Information Security Area.
- User-generated passwords must not be distributed through any channel (by oral, written or electronic distribution, etc.); passwords must be changed if there are indications that passwords or the system might be compromised – in that case a security incident must be reported
- Strong passwords must be selected, in the following way:
    - using at least 12 (twelve) characters, 14 (fourteen) characters is recommended
    - using at least one numeric character
    - using at least one uppercase and at least one lowercase alphabetic character
    - using at least one special character is recommended
    - a password should not be a dictionary word, dialectal or jargon word from any language, or any of these words written backwards
    - Passwords must not be based on personal data (e.g. date of birth, address, name of family member, etc.)
    - the last eight passwords may not be re-used
- Password must be changed as stated in 3.4

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 487

- Password must be changed at first log-on to a system
- Passwords must not be stored in an automated log-on system (e.g. macro or browser)
- Passwords used for private purposes must not be used for business purposes
- Microsoft's Password Complexity must be enabled, where available, for the domain accounts

3.6. User password management

When allocating and using user passwords, the following rules must be complied with:

- by signing the Confidentiality Statement, users also accept the obligation to keep passwords confidential, as stated by that document
- each user may use only his/her own uniquely allocated username
- each user must have the option to choose his/her own password, where applicable
- the temporary password used for first system log-on must be unique and strong, as described above
- temporary passwords must be communicated to the user in a secure manner, and user's identity must be checked beforehand
- the password management system must require the user to change the temporary password at first log-on to the system
- the password management system must require the user to select strong passwords
- the password management system must require the users to change their passwords per the schedule stated in 3.4
- the password must not be visible on the screen during log-on
- passwords created by the software or hardware manufacturer must be changed during initial installation
- files containing passwords must be stored separately from the application's system data

3.7. Review of access rights

Rights and access privileges should be reviewed using a formal or automatic control

Rule 1 - FTP Accounts in the DMZ servers should be reviewed annually

- Every account of FTP (File Transfer) on a public FTP server should be reviewed annually to assess the need to continue this account.

Rule 2 - Accounts inactive for an extended period should be disabled and deleted

- The lifetime of a dormant account must be set up to 90 days (For Brazil/LATAM, 60 days) when possible. Accounts that are inactive for more than 90 days (For Brazil/LATAM, 60 days) must be disabled. Upon notification, the account officer or the business process must validate within 15 days (For Brazil/LATAM, 30 days) the need for this account.

Additional Note
Consider exceptions in cases of personal prolonged absences (maternity, medical clearance, etc.).

3.8. Change of status or termination of contract

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 488

Upon change of employment or termination of employment, the HR area or manager must immediately inform the responsible persons who approved privileges for the employee in question.

Upon change of contractual relations with external parties who have access to systems, services and facilities, or upon expiration of the contract, contract owner must immediately inform the responsible persons who approved privileges for the external parties in question.

The access rights for all the persons who have changed their employment status or contractual relationship must immediately be removed or changed by the responsible people as defined in the previous section.

3.9. Application Development Standards

Application developers must ensure their programs contain the following security precautions. Applications:

- Must support authentication of individual users, not groups.
- Must not store passwords in clear text or in any easily reversible form.
- Must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
- Must support TACACS+, RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

4. Managing records kept on the basis of this document

- Not Applicable

5. Document management

The owner of this document is the Infrastructure and Support Department, who must check and, if necessary, update the document at least once a year.
When evaluating the effectiveness and adequacy of this document, the following criteria must be considered:

- number of incidents related to misuse of passwords by unauthorized persons
- number of incidents related to inadequate handling of passwords.

6. Appendices

- Not Applicable

7. Change history

Date	Version	Created by	Description of change
21-JAN-2014	1.0	Luiz Robson; Matthew Engler	Document creation
17-JUL -2020	2.0	Matthew Engler	Clarified the requirements on the changing of default passwords and the use of Microsoft Password Complexity. Updated to reflect 12 character requirement.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 489

stefanini
POWERING YOUR BUSINESS

POLICY ON THE USE OF CRYPTOGRAPHIC CONTROLS

Information Security Management System



Code:	ISMS-044
Version:	1.0
Date of version:	11-APR-2014
Created by:	Luiz Robson; Matthew Engler
Approved by:	Washington Souza
Confidentiality level:	Internal Use

Table of contents

1. PURPOSE, SCOPE AND USERS 3

1.1. RESPONSIBILITIES 3

2. REFERENCE DOCUMENTS 3

3. DESCRIPTION 3

3.1. USE OF CRYPTOGRAPHY 3

3.1.1. Cryptographic controls 3

3.1.2. Cryptographic keys 3

4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 4

5. DOCUMENT MANAGEMENT 4

6. APPENDICES 5

7. CHANGE HISTORY 5

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 491

1. Purpose, scope and users

The purpose of this document is to define rules for the use of cryptographic controls, as well as rules for the use of cryptographic keys, in order to protect the confidentiality, integrity and authenticity of information and to avoid user´s denial of actions performed.

This policy applies to Stefanini Employees, sub-contractors, consultants, business associates, and other workers at Stefanini, including all personnel affiliated with third parties and subsidiaries on the Stefanini infrastructure (collectively "User(s)").

1.1. Responsibilities

The Infrastructure and Support Department is responsible for preparing detailed instructions on the use of the mentioned encryption tool. Owners of individual assets to which cryptographic controls are applied are responsible for appropriate application of individual cryptographic controls.

2. Reference documents

Documents associated or linked to this one are listed below:

- ISO/IEC 27001 standard, A.10.1.1, A.10.1.2, A.18.1.5
- ISMS-001 Policy, Information Security
- ISMS-028 Policy, Information Classification and Handling
- ISMS-034 List of Legal, regulatory and other requirements

3. Description

3.1. Use of Cryptography

3.1.1. Cryptographic controls

According to *ISMS-028 Policy, Information Classification and Handling*, as well as legal and contractual obligations, the organization must protect individual systems or information through the use of cryptographic controls. Stefanini will establish guidance for the required cryptographic controls for specific systems / information.

3.1.2. Cryptographic keys

The Infrastructure and Support Department is responsible for key management as follows:

- Generation of private and public cryptographic keys
- Activation and distribution of cryptographic keys
- Definition of time limit for the use of keys and their regular updating (in accordance with the risk assessment)
- Archiving of inactive keys which are necessary for encrypted electronic archives
- Destruction of keys

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 492

Encryption keys must adhere to those algorithms that have received substantial public review and have been proven to work effectively:

- Proven, standard algorithms such as DES, Blowfish, RSA, RC5 and IDEA must be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. For example, Network Associate's Pretty Good Privacy (PGP) uses a combination of IDEA and RSA or Diffie-Hellman, while Secure Socket Layer (SSL) uses RSA encryption. Symmetric cryptosystem key lengths must be at least 128 bits. Asymmetric crypto-system keys must be of a length that yields equivalent strength.
- Stefanini's key length requirements will be reviewed annually and upgraded as technology allows.
- The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by the Global Information Security Office. Be aware that the export of encryption technologies is restricted by the U.S. Government. Residents of countries other than the United States must make themselves aware of the encryption technology laws of the country in which they reside.

Keys are managed in accordance with the above mentioned rules.

4. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Control for record protection	Retention time
Encryption Controls Guidance	ISMS Portal	Infrastructure and Support Department, Infrastructure and Support Department Representative or someone designated by him	Only the Infrastructure and Support Department Representative or someone designated by him is authorized to edit data	1 year

5. Document management

The owner of this document is the Infrastructure and Support Department that must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

- Tickets regarding the key recovery request
- Tickets regarding the key recovery request
- E.g. number of incomplete corrective actions
- E.g. number of corrective actions taken without having been recorded in a designated form

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 493

A current version of this document is available to all staff and under version control on the corporate document control system.

6. Appendices

- Not applicable

7. Change history

Date	Version	Created by	Description of change
11-APR-2014	1.0	Luiz Robson; Matthew Engler	Document creation

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 494

stefanini
POWERING YOUR BUSINESS

PHYSICAL AND ENVIRONMENTAL SECURITY POLICY

Information Security Management System



Code:	ISMS-045
Version:	3.0
Date of version:	14-JUN-2019
Updated by:	Larissa Longo
Approved by:	Washington Souza
Confidentiality level:	Internal Use

Table of contents

1. PURPOSE, SCOPE AND USERS 3
2. REFERENCE DOCUMENTS 3
3. DESCRIPTION 3
3.1. DEFINITIONS 3
3.2. RESPONSIBILITIES 3
3.3. SECURED AREAS 4
3.4. SECURE PHYSICAL PERIMETER 4
3.5. PHYSICAL ACCESS CONTROL 4
3.6. WORKING IN SECURED AREAS 4
3.7. PROTECTION AGAINST EXTERNAL ENVIRONMENTAL THREATS 5
3.8. BUSINESS CONTINUITY PLAN 5
4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 5
5. DOCUMENT MANAGEMENT 6
6. APPENDICES 6
7. CHANGE HISTORY 6

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 496

1. Purpose, scope and users

This procedure is established to protect information assets, providing guarantees in the physical and environmental security for the facility.

It applies to all facilities Stefanini linked directly or indirectly to the ISMS.

2. Reference documents

Documents associated or linked are listed below:

- ISO/IEC 27001 standard, A.8.2.3, A.11.1, A.11.1.4
- ISMS-001 Policy, Information Security
- ISMS-021 Procedure, Risk Treatment Plan
- ISMS-031 Policy, Business Continuity Management
- ISMS-036 Procedure, Access Control, Monitoring and People Identification
- Business Continuity Plan

3. Description

3.1. Definitions

Data center: Area within Stefanini facilities where the data storage center, network services and other control or monitoring of the Information Security management System occurs. By default, a data center is a Secured Area.

Secured Area: A room containing production infrastructure or items of value (identified via risk evaluation) to Stefanini, requiring that it be secured against theft and intrusion. This includes server rooms, network rooms, rooms containing datacenter support equipment (e.g. UPS) and shipping / receiving docks. In a Stefanini facility, the security areas are shown on a “Security Area Map”.

Physical access control – Credentials, biometrics, keys or any other way of authentication to give or not access to a secured area.

Service provider or contracted person –Company or Staff providing a service to Stefanini, but is not an employee of Stefanini.

3.2. Responsibilities

The Information Security Manager and Facility Management is responsible for defining and addressing risks to Stefanini facilities and establishing physical security controls according to the local profile and the risks identified.

The Asset Owner / Manager will support the Security Committee to define physical protection necessary to protect information assets in their area of responsibility.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 497

The Security Committee must analyse areas identified in collaboration with the owners of the assets to determine the controls and guidelines needed to manage, reduce or eliminate the identified level of risk (threat) to information assets .

All users are required to comply with the requirements of this procedure. They must also take an active role in protecting Stefanini facilities and must report security violations to the Information Security Manager.

3.3. Secured Areas

Areas where Information assets are processed should be assessed for their level of risk or threat. Areas with high risk threat will be identified as "secured areas".

Controls to ensure adequate protection for the areas identified must be addressed. This should include physical protection (barriers). Appropriate access controls will be established to ensure that only authorized personnel have access to the area.

Offices, rooms and facilities that support the activities of business-critical information must be identified and secured.

Activities and users within a secured area should be supervised.

3.4. Secure physical perimeter

Areas requiring physical security perimeters should be determined during the risk assessment process.

It must ensure that:

- Security perimeters controls provide adequate protection to the level of the threat to information assets or business sector.
- Access to the facility is restricted to authorized personnel.

3.5. Physical access control

Service providers or contracted person access must be registered prior to working in a Stefanini facility.

While service providers are working in secured areas, access to sensitive information is restricted. If the information cannot be satisfactorily secured, a Stefanini employee must accompany the provider at all times.

No visitors are allowed in the secured areas, unless express permission is given.

Visitors with permission to access secured areas must sign in at a visitor log.

Access Control Requirements:

- Each employee must be authenticated by the physical access control to enter through any door controlled within the premises of Stefanini.
- Employees must not use their access to open access doors to another person or let other people get through with their authentication.
- When a user completes their working relationship with Stefanini, all security codes known, physical access and/or provisions should be disabled or changed immediately.

The Data Center Room and file areas and other locations where confidential information are handled or stored must be locked.

3.6. Working in secured areas

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 498

Working in secured areas requirements:

- Doors to secured areas should be locked.
- Only users who have received access (either keys, biometric access) should enter the secured areas, unless an authorized staff member accompanies them. Any unauthorized person should not be left alone in the secured area.
- All recording medium such as cameras, video, audio or other equipment are prohibited except when they have been expressly and formally approved by the Information Security Manager.
- Staff who have received keys to access secure areas must not lend it to any other staff.
- The work stations in secured areas must be locked when not in use.
- In secured areas it is not allowed to:
    - Plug any electrical device into a power supply unless specifically authorized to do so;
    - Touch or in any other way tamper with any equipment installed in secure areas unless specifically authorized to do so;
    - Connect any device to a network unless specifically authorized to do so;
    - Store flammable materials or equipment;
    - Use any kind of heating devices;
    - Smoke, eat or drink.

3.7. Protection against external environmental threats

The following environmental safety measures are implemented:

- Adequate equipment for the detection OR extinguishing of a fire;
- Adequate equipment for maintaining room temperature;
- For data centers, adequate equipment or process for the monitoring of room temperature and alerting if outside of defined thresholds;
- Equipment should be protected against environmental changes in power;
- Locate power cables away from foot traffic to minimize ICT staff tripping or knocking power cables out of ICT equipment;
- Installation of appropriate back up emergency lighting in case of a mains power failure;
- Contingency plan on such situation.

3.8. Business Continuity Plan

For events related to Business Continuity, apply the *ISMS-031 Policy, Business Continuity Management* and the actions of Business Continuity Plan.

4. Managing records kept on the basis of this document

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 499

- Not applicable

5. Document management

The owner of this document is the Information Security Manager, who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria must be considered:

- Number of incidents related to this policy
- Audits results

A current version of this document is available to all staff and under version control on the corporate document control system.

6. Appendices

- Not applicable

7. Change history

Date	Version	Created by	Description of change
22-JAN-2014	1.0	Luiz Robson	Document creation
23-AUG-2014	2.0	Matthew Engler	Added room temperature monitoring
14-JUN-2019	3.0	Larissa Longo	Updated the mandatory fire detection equipment

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 500

SECURE DEVELOPMENT POLICY

Information Security Management System



Code:	ISMS-046
Version:	2.0
Date of version:	20-AUG-2020
Created by:	Licsileth Palma
Approved by:	Washington Souza
Confidentiality level:	Internal Use

Table of contents

1. PURPOSE, SCOPE AND USERS 3
2. REFERENCE DOCUMENTS 3
3. DESCRIPTION 3
3.1 POLICY STATEMENT 3
3.1.1 RISK ASSESSMENT FOR THE DEVELOPMENT PROCESS 3
3.1.2 SECURING THE DEVELOPMENT ENVIRONMENT 4
3.1.3 SECURE ENGINEERING PRINCIPLES 4
3.1.4 SECURITY REQUIREMENTS 4
3.1.5 SECURITY REQUIREMENTS RELATED TO PUBLIC NETWORKS 4
3.1.6 CHECKING AND TESTING THE IMPLEMENTATION OF SECURITY REQUIREMENTS 4
3.1.7 SOFTWARE DEVELOPMENT 5
3.1.7.1 Repository 5
3.1.7.2 Version Control 5
3.1.7.3 Change Control 5
3.1.8 PROTECTION OF TEST DATA 5
3.1.9 REQUIRED SECURITY TRAINING 5
3.1.10 SUPPLIER 5
4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 6
5. DOCUMENT MANAGEMENT 6
6. APPENDICES 6
7. CHANGE HISTORY 7

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 502

1. Purpose, scope and users

The purpose of this policy is to describe the operation followed by Stefanini for managing the security of vital information and/or material while using or developing Information systems.

This policy applies to Stefanini Employees, sub-contractors, consultants, business associates, and other workers at Stefanini, including all personnel affiliated with third parties and subsidiaries on the Stefanini infrastructure (collectively “User(s)”).

2. Reference documents

Documents associated or linked are listed below:

- ISO/IEC 27001 standard, A.14.1.2, A.14.1.3, A.14.2.1, A.14.2.2, A.14.2.5, A.14.2.6, A.14.2.8, A.14.2.9, A.14.3.1
- ISMS-001 Information Security Policy
- ISMS-010 Acceptable use Policy
- ISMS-011 Change management policy
- ISMS-013 Training and Awareness procedure
- ISMS-019 Risks Identification and Assessment Procedure
- ISMS-020 Risk Analysis Procedure
- ISMS-033 Configuration Management Procedure
- ISO/IEC 20000 standard

3. Description

3.1 Policy Statement

3.1.1 Risk assessment for the development process

In addition to the risk assessment performed according to the Risk Assessment and Risk Treatment Plan, the Information Security Manager must periodically perform the assessment of the following:

- Risks related to unauthorized access to the development environment
- Risks related to unauthorized changes to the development environment
- Technical vulnerabilities of the IT systems used in the organization
- Risks a new technology might bring if used in the organization

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 503

3.1.2 Securing the development environment

In addition to the Development Environment Security, the Operation must following the rules as described in the “Service Planning” and “Release and Deployment Management”; both are ISO 20000.

3.1.3 Secure engineering principles

The Information Security Manager must keep updated the roles and principles for secure information system engineering. The principles are:

- ISMS-001 Information Security Policy
- ISMS-002 Information Security Manual
- ISMS-010 Acceptable use Policy
- ISMS-041 Communications and Operations Security

3.1.4 Security Requirements

When acquiring new information systems or developing or changing existing ones, the Information Security Manager must document the security requirements according to the requirements specifications of each project or service.

3.1.5 Security Requirements Related to public networks

The Information Security Manager is responsible for defining security controls related to information / application services passing over public networks:

- Description of authentication systems to be used
- Description of how confidentiality and integrity of information is to be ensured
- Description of how non-repudiation of actions will be ensured

The Information Security Manager is responsible for defining controls for online transactions, which must include the following:

- How misrouting will be prevented
- How incomplete data transmission will be prevented
- How unauthorized message alteration will be prevented
- How unauthorized message duplication will be prevented
- How unauthorized data disclosure will be prevented

3.1.6 Checking and testing the implementation of security requirements

The Information Security Manager is responsible for defining the methodology, responsibilities and the timing of checking whether all the security requirements from the Security Requirements Specifications have been met, and whether the system is acceptable for production.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 504

3.1.7 Software Development

3.1.7.1 Repository

All the information about the repository you can find in ISMS-033 Configuration Management Procedure.

3.1.7.2 Version Control

All the information about the repository you can find in ISMS-033 Configuration Management Procedure and in the documents of ISO 20000 Methodology (SMS-TEM-10 Configuration Items Plan_EN, SMS-POL-07 Software Maintenance Policy_EN, SMS-POL-08 Documents Maintenance Policy_EN, SMS-PRO-06 Software Maintenance Procedure_EN, SMS-PRO-07 Documents Maintenance Procedure_EN).

3.1.7.3 Change Control

All the information about the repository you can find in ISMS-033 Configuration Management Procedure and in the documents of ISO 20000 Methodology (SMS-TEM-10 Configuration Items Plan_EN, SMS-POL-07 Software Maintenance Policy_EN, SMS-POL-08 Documents Maintenance Policy_EN, SMS-PRO-06 Software Maintenance Procedure_EN, SMS-PRO-07 Documents Maintenance Procedure_EN).

3.1.8 Protection of Test Data

Confidential data, as well as data can be related to individual persons must not be used as test data. Exceptions may be approved only by Operation Manager and Information Security Manager, in which case both must define how such test data are protected.

3.1.9 Required Security Training

The Information Security Manager defines the level of security skills and knowledge required for the development process and proposes the trainings to Human Resources of Stefanini. The Operation Manager, HR and the Information Security Manager include appropriate trainings in the Training and Awareness Plan.

3.1.10 Supplier

Where a contracted supplier is used, the responsible organization should ensure that a secure development methodology is used. The supplier should allow for security auditing of development practices.

Note: For Stefanini Colombia, all this information is in:

- Safe Code Development Policy IN-DD-24,
- Visual Basic programming standards IN-DD-02,
- Standards for programming in databases IN-DD-03,
- Coding Standards in Power Builder IN-DD-04,
- Architecture and programming standards in .NET IN-DD-07,
- Java programming standards IN-DD-08,
- Structuring standards in Cognos IN-DD-09,
- SharePoint Development Standards.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 505

- Analysis DC FR-DD-07,
- Project Design FR-DD-16

4. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
Security Requirements	Stefanini´s portal	Information Security Manager or someone designated by him	Only Information Security Manager or someone designated by him or personnel with authorized access is authorized to edit data	1 year
Information Security Request	Stefanini´s portal	Top Management Representative	Only Top Management Representative has the right to make entries into and changes to the Secure Development Policy.	1 year
Asset, Risks and Classification	Risks Spreadsheet	Top Management Representative	Only Top Management Representative has the right to make entries into and changes to the Secure Development Policy.	1 year

5. Document management

The owner of this document is the Information Security Manager, who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria must be considered:

- The number of incidents with access denied
- The number of incidents with password problems

A current version of this document is available to all staff and under version control on the corporate document control system.

6. Appendices

- Not applicable

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 506

7. Change history

Date	Version	Created by	Description of change
22-MAR-2014	1.0	Rodrigo Ricci	Document creation
20-AGO-2020	2.0	Licsileth Palma	Included for Colombia Standards, procedures, and instructions.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 507

MOBILE DEVICE AND TELEWORKING POLICY

Information Security Management System



Code:	ISMS-047
Version:	1.0
Date of version:	27-JAN-2014
Created by:	Rodrigo Ricci
Approved by:	Washington Souza
Confidentiality level:	Internal Use

Table of contents

1. PURPOSE, SCOPE AND USERS 3
2. REFERENCE DOCUMENTS 3
3. DESCRIPTION 3
3.1. MOBILE COMPUTING – INTRODUCTION 3
3.2. BASIC RULES 3
3.3. TELEWORKING 4
4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 5
5. DOCUMENT MANAGEMENT 5
6. APPENDICES 5
7. CHANGE HISTORY 5

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 509

1. Purpose, scope and users

The purpose of this document is to ensure security measures and controls are implemented when using mobile computing devices both within and outside of the organization's premises.

This policy applies to Stefanini Employees, sub-contractors, consultants, business associates, and other workers at Stefanini, including all personnel affiliated with third parties and subsidiaries on the Stefanini infrastructure (collectively “User(s)”).

2. Reference documents

- ISO/IEC 27001 standard, A.6.2, A.11.2.6
- ISMS-001 Policy, Information Security
- ISMS-010 Policy, Acceptable use
- ISMS-022 Policy, Clear desk and clear screen
- ISMS-028 Policy, Information Classification and Handling

3. Description

3.1. Mobile Computing – Introduction

Mobile Computing is defined as "taking a computer and all necessary files and software out into the field". Mobile computing equipment includes all kinds of portable computers, mobile phones, smart phones, memory cards and other mobile equipment used for storage, processing and transferring of data.

The mobile equipment may be taken off-premises only after obtaining proper authorization.

3.2. Basic Rules

Special care should be taken when mobile computing equipment is placed in vehicles (including cars), public spaces, hotel rooms, meeting places, conference centers, and other unprotected areas outside the organization's premises.

The person taking mobile computing equipment off-premises must follow these rules:

- Mobile computing equipment carrying important, sensitive or critical information must not be left unattended and, if possible, should be physically locked away. Special locks should be used where applicable to physically secure the equipment.
- When using mobile computing equipment in public places, the user must take care that data cannot be read by unauthorized persons.
- Updates of patches and other system settings, where applicable, are performed when the mobile computing device is connected to the Stefanini network.
- Protection against malicious code is installed and updated on mobile computing devices, when available. The user shall not deactivate any malicious code protections.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 510

- The person using mobile computing equipment outside the Stefanini network will need to update modified files within network folders and / or backup the system per the Acceptable Use Policy.
- Care must be taken when connecting to communication networks and data exchange. Data transferred via wired and wireless communications is subject to interception. Restricted information may only be transferred over the network via a secured communication path (VPN, SSL, etc.)
- Restricted Information on portable computers must be encrypted. Confidential information on portable computers is recommended to be encrypted.
- Protection of sensitive data must be implemented in accordance with the *ISMS-028 Policy, Information Classification and Handling*.
- In case mobile computing equipment is left unattended, rules for unattended user equipment must be applied in applied in line with the *ISMS-022 Policy, Clear desk and clear screen*.

The Human Resource area is responsible for training and raising the awareness of persons who are using mobile computing equipment outside the organization's premises.

3.3. Teleworking

Teleworking means that information and communication equipment is used to enable employees to perform their work outside a Stefanini facility. Teleworking does not include the use of mobile phones outside the organization's premises.

Each manager implicitly authorizes Teleworking when the equipment is requested. The manager should define the work permitted, the hours of work, the classification of information that may be held and the internal systems that the teleworker is authorized to access.

Infrastructure and Support Departments are responsible for preparing plans and procedures to ensure the following:

- Protection of mobile computing equipment as specified in the previous section.
- Prevention of unauthorized access by persons living or working on the location where the teleworking activity is performed.
- Appropriate configuration of the local network used for connecting to the Internet.
- Protection of the organization's intellectual property rights, either for software or other materials that may be protected by intellectual property rights.
- Process for returning of data and equipment in the case of termination of employment.
- Ensuring off-premises locations have been evaluated properly for risk and controls implemented as necessary.
- Permitted and forbidden types of activities.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 511

4. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Control for record protection	Retention time
Authorization for teleworking	Service Desk Ticketing System	N/A	Inherent System Controls	Records are stored for a period of 2 years.
Operational Procedures for teleworking	Corporate Document Control System	N/A	Only the Designated by Management Representative can edit and publish new version	As long as required.

5. Document management

The owner of this document is the Top Management Representative, who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria must be considered:

- number of incidents related to taking mobile computing equipment outside the organization's premises without authorization
- number of incidents related to unauthorized access to mobile computing equipment outside the organization's premises

A current version of this document is available to all staff and under version control on the corporate document control system.

6. Appendices

- Not applicable.

7. Change history

Date	Version	Created by	Description of change
27-JAN-2014	1.0	Rodrigo Ricci	Document creation

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 512

SUPPLIER SECURITY STANDARD

Information Security Management System



Code:	ISMS-049
Version:	2.1
Date of version:	08-SEP-2015
Created by:	Matthew Engler
Approved by:	Washington Souza
Confidentiality level:	Internal Use

Table of contents

1. PURPOSE, SCOPE AND USERS 3
2. REFERENCE DOCUMENTS 3
3. DESCRIPTION 3
3.1. SUPPLIER SECURITY STANDARDS 3
3.1.1. Responding to These Standards 3
3.2. GENERAL SECURITY 4
3.3. PHYSICAL SECURITY 4
3.4. NETWORK SECURITY 4
3.5. HOST SECURITY 5
3.6. WEB SECURITY 5
3.7. CRYPTOGRAPHY 5
4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 6
5. DOCUMENT MANAGEMENT 6
6. APPENDICES 6
7. CHANGE HISTORY 6

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 514

1. Purpose, scope and users

This document defines the minimum security criteria that a Supplier who will host Stefanini Confidential or Restricted data must meet in order to be considered for use. This standard can be provided to SUPPLIERs that are either being considered for use by Stefanini or have already been selected for use.

These Standards are subject to additions and changes without warning by the Information Security Management Team.

This policy applies to any use of Suppliers by Stefanini independent of where data may be hosted.

2. Reference documents

Documents associated or linked tare listed below:

- ISO/IEC 27001 standard, 4.1, 4.2, 7.4, A.5.1.1, A.7.1.2, A.7.2.2, A.7.3.1., A.15
- ISMS-001 Policy, Information Security
- ISMS-024 Policy, Supplier Security

3. Description

3.1. Supplier Security Standards

As part of the Supplier selection process, the Vendor must demonstrate compliance with the Standards listed below. The Information Security Team will closely review the vendor responses, and will suggest remediation measures in any areas that fall short of the minimum security criteria. The Information Security Team approval of any given Supplier resides largely on the vendor's response to this standard.

3.1.1. Responding to These Standards

The Information Security Team is looking for explicitly detailed, technical responses to the following statements and questions. Suppliers should format their responses directly beneath the Standards (both questions and requirements) listed below. In addition, please include any security whitepapers, technical documents, or policies that you may have.

Answers to each Guideline should be specific and avoid generalities, examples:

- Bad: "We have hardened our hosts against attack."
- Good: "We have applied all security patches for Windows 2000 as of 8/31/2000 to our servers. Our Administrator is tasked with keeping up-to-date on current vulnerabilities that may affect our environment, and our policy is to apply new patches during our maintenance period (2300hrs, Saturday) every week. Critical updates are implemented within 24 hours. A complete list of applied patches is available to Stefanini."
- Bad: "We use encryption."

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 515

- Good: "All communications between our site and Stefanini will be protected by IPSec ESP Tunnel mode using 168-bit TripleDES encryption, SHA-1 authentication. We exchange authentication material via either out-of-band shared secret, or PKI certificates."

3.2. General Security

Stefanini reserves the right to periodically audit the Stefanini application infrastructure to ensure compliance with the Supplier Security Policy and these Standards. Non-intrusive network audits (basic portscans, etc.) may be done randomly, without prior notice. More intrusive network and physical audits may be conducted on site with 24 hours' notice.

The Supplier must provide a proposed architecture document that includes a full network diagram of the Stefanini Application Environment, illustrating the relationship between the Environment and any other relevant networks, with a full data flowchart that details where Stefanini data resides, the applications that manipulate it, and the security thereof.

The Supplier must be able to immediately disable all or part of the functionality of the application should a security issue be identified.

3.3. Physical Security

The equipment hosting the application for Stefanini must be located in a physically secure facility, which requires badge access at a minimum.

The infrastructure (hosts, network equipment, etc.) hosting the Stefanini application must be located in a locked cage-type environment.

Stefanini shall have final say on who is authorized to enter any locked physical environment, as well as access the Stefanini Application Infrastructure.

The Supplier must disclose who amongst their personnel will have access to the environment hosting the application for Stefanini.

Stefanini's Information Security Team requires that the Supplier disclose their Supplier background check procedures and results prior to the Information Security Manager granting approval for use of a Supplier.

3.4. Network Security

The network hosting the application must be air-gapped from any other network or customer that the Supplier may have. This means the Stefanini application environment must use separate hosts, and separate infrastructure.

How will data go between Stefanini and the Supplier? Keep in mind the following two things:

- If Stefanini will be connecting to the Supplier via a private circuit (such as frame relay, etc.), then that circuit must terminate on the Stefanini extranet, and the operation of that circuit will come under the procedures and policies that govern the Stefanini Partner Network Management Group.
- If, on the other hand, the data between Stefanini and the SUPPLIER will go over a public network such as the Internet, appropriate firewalling technology must be deployed by the SUPPLIER, and the traffic between Stefanini and the Supplier must be protected and authenticated by cryptographic technology (See Cryptography below).

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 516

3.5. Host Security

The Supplier must disclose how and to what extent the hosts (UNIX, Windows, etc.) comprising the Stefanini application infrastructure has been hardened against attack. If the Supplier has hardening documentation for the CAI, provide that as well.

If requested, the Supplier must provide a listing of current patches on hosts, including host OS patches, web servers, databases, and any other material application.

Information on how and when security patches will be applied must be provided. How does the Supplier keep up on security vulnerabilities, and what is the policy for applying security patches?

The Supplier must disclose their processes for monitoring the integrity and availability of those hosts.

The Supplier must provide information on their password policy for the Stefanini application infrastructure, including minimum password length, password generation guidelines, and how often passwords are changed.

Stefanini cannot provide internal usernames/passwords for account generation, as the company is not comfortable with internal passwords being in the hands of third parties. With that restriction, how will the Supplier authenticate users? (e.g., LDAP, Netegrity, Client certificates.)

The Supplier must provide information on the account generation, maintenance and termination process, for both maintenance as well as user accounts. Include information as to how an account is created, how account information is transmitted back to the user, and how accounts are terminated when no longer needed.

3.6. Web Security

At Stefanini's discretion, the Supplier may be required to disclose the specific configuration files for any web servers and associated support functions (such as search engines or databases).

Please disclose whether, and where, the application uses Java, Javascript, ActiveX, PHP or SUPPLIER (active server page) technology.

What language is the application back-end written in? (C, Perl, Python, VBScript, etc.)

Please describe the Supplier process for doing security Quality Assurance testing for the application. For example, testing of authentication, authorization, and accounting functions, as well as any other activity designed to validate the security architecture.

Has the Supplier done web code review, including CGI, Java, etc, for the explicit purposes of finding and remediating security vulnerabilities? If so, who did the review, what were the results, and what remediation activity has taken place? If not, when is such an activity planned?

3.7. Cryptography

The Stefanini application infrastructure cannot utilize any "homegrown" cryptography – any symmetric, asymmetric or hashing algorithm utilized by the Stefanini application infrastructure must utilize algorithms that have been published and evaluated by the general cryptographic community.

Encryption algorithms must be of sufficient strength to equate to 168-bit TripleDES.

Preferred hashing functions are SHA-1 and MD-5.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 517

Connections to the Supplier utilizing the Internet must be protected using any of the following cryptographic technologies: IPSec, SSL, SSH/SCP, PGP.

If the Stefanini application infrastructure requires PKI, please contact the Information Security Team for additional guidance.

4. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
Supplier Security Standard Review	Electronic: Shared Drive; Paper: Locked Cabinets	Information Security Manager	Only authorized personnel have access.	5 years after the termination of the contract

5. Document management

The owner of this document is the Information Security Team, who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria must be considered:

- number of incidents related to supplier failure to perform a function as documented by the supplier in this standard
- number of incidents related to a supplier failure by a function NOT covered by this standard

A current version of this document is available to all staff and under version control on the corporate document control system.

6. Appendices

- Not applicable

7. Change history

Date	Version	Created by	Description of change
01-MAY-2014	1.0	Matthew Engler	Document creation
23-AUG-2014	2.0	Matthew Engler	Removed “or have access to” under purpose
08-SEP-2015	2.1	Matthew Engler	Removed the requirement that suppliers respond specifically to this document.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 518

NON-EXPIRING PASSWORD POLICY

Information Security Management System



Code:	ISMS-050
Version:	1.0
Date of version:	02-MAY-2014
Created by:	Matthew Engler
Approved by:	Washington Souza
Confidentiality level:	Internal Use

Table of contents

1. PURPOSE, SCOPE AND USERS 3
2. REFERENCE DOCUMENTS 3
3. DESCRIPTION 3
4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 3
5. DOCUMENT MANAGEMENT 3
6. APPENDICES 4
7. CHANGE HISTORY 4

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 520

1. Purpose, scope and users

This policy allows for non-expiring passwords to be used for the sole purpose of running or executing applications on an on-going basis. This policy should not be confused with password policies that govern the use and management of individual user IDs and passwords.

This policy applies to server equipment owned and/or operated by Stefanini and to servers registered under any Stefanini-owned network domain where a user ID is required for application functionality.

2. Reference documents

- ISO/IEC 27001 standard, A.9.4.2, A.9.4.4, A.14.2.1
- ISMS-001 Policy, Information Security
- ISMS-043 Policy, Account and Password

3. Description

The use of non-expiring passwords, in conjunction will application user IDs, is permitted for the express purpose of supporting applications under the following provisions:

- Each application is assigned a unique application user ID and password. Application user IDs and passwords may not be shared among multiple applications.
- The application user ID may not be used by individual user.
- The application user ID must be restricted to the minimum access level required for application function.
- The application user ID cannot provide interactive system log-on privileges.
- The application owner is responsible for the distribution and management of the application user ID and password.

4. Managing records kept on the basis of this document

- Not Applicable

5. Document management

The owner of this document is the Infrastructure and Support Department, who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria must be considered:

- number of incidents related to misuse of passwords by unauthorized persons

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 521

6. Appendices

- Not Applicable

7. Change history

Date	Version	Created by	Description of change
02-MAY-2014	1.0	Matthew Engler	Document creation

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 522

stefanini
POWERING YOUR BUSINESS

SERVER / SYSTEM SECURITY POLICY

Information Security Management System



Code:	ISMS-051
Version:	2.0
Date of version:	04-SEP-2014
Created by:	Matthew Engler
Approved by:	Washington Souza
Confidentiality level:	Internal Use

Table of contents

1. PURPOSE, SCOPE AND USERS 3
2. REFERENCE DOCUMENTS 3
3. DESCRIPTION 3
3.1. Ownership and Responsibilities 3
3.2. General Configuration Guidelines 4
3.3. New Installations and Change Management Procedures 5
3.4. Monitoring 5
3.5. Compliance 5
3.6. Equipment Outsourced to External Service Providers 6
4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 6
5. DOCUMENT MANAGEMENT 6
6. APPENDICES 6
7. CHANGE HISTORY 7

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 524

1. Purpose, scope and users

The *Server / System Security Policy* establishes standards for the base configuration of internal server equipment that is owned and/or operated by Stefanini. This includes all equipment owned and/or operated by Stefanini with access available from the public Internet. This policy is designed to minimize the potential exposure to Stefanini from the loss of confidential / restricted data, intellectual property, damage to public image etc., which may follow from unauthorized use of Stefanini resources.

This policy applies to:

- Server equipment owned and/or operated by Stefanini and to servers registered under any Stefanini-owned network domain.
- All equipment or devices deployed in a DMZ owned and/or operated by Stefanini (including hosts, routers, switches, etc.) and/or registered in any Domain Name System (DNS) domain owned by Stefanini. This includes systems deployed in a DMZ-like solution, such as a reverse or application proxy.

This policy also covers any host device outsourced or hosted at external/third-party service providers, if that equipment resides in a Stefanini-owned domain or appears to be owned by Stefanini.

All new equipment which falls under the scope of this policy must be configured according to the referenced configuration documents, unless a waiver is obtained from the Information Security Manager. All existing and future equipment deployed on Stefanini's un-trusted networks must comply with this policy.

2. Reference documents

- ISO/IEC 27001 standard, A.9.4.1, A.11.2.1, A.13.1.3, A.14.1, A.14.2, A.14.3, A.14.2.2, A.14.2.3, A.14.2.8, A.18.2.3
- ISMS-001 Policy, Information Security
- ISMS-004 Procedure, Backup system [Site Specific]
- ISMS-020 Procedure, Risk Analysis
- ISMS-023 Procedure, Incident Management
- ISMS-043 Policy, Account and Password

3. Description

3.1. Ownership and Responsibilities

All Servers/Systems deployed at Stefanini must be owned by a Support Group that is responsible for system administration. Approved server configuration guides must be established and maintained by each Support Group, based on business needs and approved by the Information Security Management Team. Support Groups must monitor configuration compliance and implement an exception policy tailored to their

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 525

environment. Each Support Group must establish a process for changing the configuration guides, which includes review and approval by the Information Security Management Team.

- Servers/Systems must be registered as part of Configuration Management. At a minimum, the following information is required to positively identify the point of contact:
  - Server contact(s) and location, and a backup contact
  - Hardware and Operating System/Version
  - Main functions and applications, if applicable
  - Password groups for privileged passwords, if applicable
- Information on a system must be kept up-to-date.
- Configuration changes for production servers must follow the appropriate change management procedures.
- Network interfaces must have appropriate Domain Name Server records (minimum of A and PTR records).
- Password groups must be maintained in accordance with the *ISMS-043 Policy, Account and Password*.
- Immediate access to equipment and system logs must be granted to members of the Global Information Security Office upon demand, per *ISMS-020 Procedure, Risk Analysis*.

3.2. General Configuration Guidelines

- Hardware, operating systems, services and applications should be approved by the Information Security Management Team as part of the pre-deployment review phase.
- Operating System configuration must be in accordance with approved guidelines.
- Services and applications that will not be used must be disabled where practical.
- Access to services must be logged and/or protected through access-control methods such as TCP Wrappers, if possible.
- All security patches/hot-fixes recommended by the hardware/software vendor and the Information Security Management Team must be installed as soon as practical, the only exception being when immediate application would interfere with business requirements. This applies to all services installed, even though those services may be temporarily or permanently disabled.
- Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will do.
- Always use standard security principles of least required access to perform a function.
- Do not use root access when a non-privileged account will do.
- If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 526

IPSec). For systems residing in the DMZ, remote administration must be performed over secure channels (e.g., encrypted network connections using SSH or IPSEC) or console access independent from the DMZ networks. Where a methodology for secure channel connections is not available, one-time passwords (DES/SofToken) must be used for all access levels.

- Servers/Systems must be physically located in an access-controlled environment.
- Servers/Systems are specifically prohibited from operating from uncontrolled cubicle areas.
- Servers/Systems must be designed with redundancy to meet the required availability.
- If the server is hosting a web application which requires personal credentials be transported between the user and the server, it is required that an SSL Certificate be installed on the system to prevent data leakage.

3.3. New Installations and Change Management Procedures

All new installations and changes to the configuration of existing equipment and applications must follow the following policies/procedures:

- New installations must be approved by appropriate management and follow a Server Build Process.
- Configuration changes must follow the Change Management (CM) Procedures.
- The Information Security Management Team must be invited to perform system/application audits prior to the deployment of new services.
- The Information Security Management Team must be engaged, either directly or via CM, to approve all new deployments and configuration changes.

3.4. Monitoring

- All security-related events on critical systems or systems containing Restricted data must be logged and audit trails saved as follows:
  - All security related logs will be kept online for a minimum of 1 week.
  - Backups will be maintained per *ISMS-004 Procedure, Backup system*.
- Security-related events will be reported to the Information Security Management Team per *ISMS-023 Procedure, Incident Management*, who will review logs and report incidents to Top management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
  - Port-scan attacks
  - Evidence of unauthorized access to privileged accounts
  - Anomalous occurrences that are not related to specific applications on the host.

3.5. Compliance

- Audits will be performed on a regular basis by authorized organizations within Stefanini.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 527

- Audits will be managed by the Infrastructure and Support Departments and the Information Security Management Team, in accordance with the *ISMS-020 Procedure, Risk Analysis*. The Information Security Management Team will filter findings not related to a specific Support Group and then present the findings to the appropriate support staff for remediation or justification.
- Every effort will be made to prevent audits from causing operational failures or disruptions.

3.6. Equipment Outsourced to External Service Providers

The responsibility for the security of the equipment deployed by external service providers must be clarified in the contract with the service provider and security contacts, and escalation procedures documented. Contracting departments are responsible for third party compliance with this policy.

4. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Control for record protection	Retention time
Asset Information	Configuration Management System	N/A	Inherent System Controls	Records are stored for the life of the system plus 1 year.
Configuration Guidelines	ICT Shared Drives; System Templates	Infrastructure and Support Departments	Inherent System Controls	As long as required.

5. Document management

The owner of this document is the Top Management Representative, who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria must be considered:

- number of Incidents related to a security breach as a result of a system misconfiguration
- number of deployed systems which do not meet configuration guidelines

A current version of this document is available to all staff and under version control on the corporate document control system.

6. Appendices

- Not applicable.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 528

7. Change history

Date	Version	Created by	Description of change
29-MAY-2014	1.0	Matthew Engler	Document creation
04-SEP2014	2.0	Matthew Engler	Added redundancy requirement; change Server to "Servers/Systems"

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 529

TECHNOLOGY LAB SECURITY POLICY

Information Security Management System



Code:	ISMS-052
Version:	1.0
Date of version:	09-JUN-2014
Created by:	Matthew Engler
Approved by:	Washington Souza
Confidentiality level:	Internal Use

Table of contents

1. PURPOSE, SCOPE AND USERS 3
2. REFERENCE DOCUMENTS 3
3. DESCRIPTION 3
3.1. OWNERSHIP AND RESPONSIBILITIES 3
3.2. GENERAL CONFIGURATION GUIDELINES 4
4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 5
5. DOCUMENT MANAGEMENT 5
6. APPENDICES 6
7. CHANGE HISTORY 6

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 531

1. Purpose, scope and users

The *Technology Lab Security Policy* establishes information security requirements for Stefanini Technology Labs to ensure that Stefanini confidential information and technologies are not compromised, and that production services and other Stefanini interests are protected from lab activities.

This policy applies to all internally connected labs, Stefanini Employees and third parties who access Stefanini's labs.

A Technology Lab is any non-production environment, intended specifically for developing, demonstrating, training and/or testing of a product.

2. Reference documents

- ISO/IEC 27001 standard, A.9.4.1, A.12.1.4, A.13.1.3, A.14.1, A.14.2, A.14.3, A.14.2.2, A.14.2.8, A.14.3.1, A.18.2.3
- ISMS-001 Policy, Information Security
- ISMS-039 Policy, Anti-Virus_Anti-Malware Software
- ISMS-036 Procedure, Facility Access Control and Monitoring [Site Specific]
- ISMS-043 Policy, Account and Password

3. Description

3.1. Ownership and Responsibilities

- Technology Lab owning organizations are responsible for assigning lab managers, a point of contact (POC), and a back-up POC for each lab. Lab owners must maintain up-to-date POC information with the Information Security Management Team or the Support and Infrastructure Department. Lab managers or their backup must be available around-the-clock for emergencies, otherwise actions will be taken without their involvement.
- Technology Lab managers are responsible for the security of their labs and the lab's impact on the corporate production network and any other networks. Lab managers are responsible for adherence to this policy and associated processes. Where policies and procedures are undefined, Technology Lab managers must do their best to safeguard Stefanini from security vulnerabilities.
- Technology Lab managers are responsible for the lab's compliance with all Stefanini security policies. The following are particularly important: *ISMS-043 Policy, Account and Password*, *ISMS-039 Policy, Anti-Virus_Anti-Malware Software*, and *ISMS-036 Procedure, Facility Access Control and Monitoring*.
- The Lab Manager is responsible for controlling lab access. Access to any given lab will only be granted by the lab manager or designee, to those individuals with an immediate business need within the lab, either short-term or as defined by their ongoing job function. This includes

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 532

continually monitoring the access list to ensure that those who no longer require access to the lab have their access terminated.

- The Network Team must maintain a firewall device between the corporate production network and all lab equipment.
- The Network team and/or the Information Security Management Team reserve the right to interrupt lab connections that impact the corporate production network negatively or pose a security risk.
- The Network team must record all lab IP addresses, which are routed within Stefanini networks, in Enterprise Address Management database along with current contact information for that lab.
- Any lab that wants to add an external connection must provide documentation to the Information Security Management team with business justification, the equipment, and the IP address space information. The Information Security Management team will review for security concerns and must approve before such connections are implemented or presented to the Change Management Process.
- All user passwords must comply with *ISMS-043 Policy, Account and Password*. In addition, individual user accounts on any lab device must be deleted when no longer authorized within three (3) days. Group account passwords on lab computers (UNIX, windows, etc.) must be changed quarterly (once every 3 months). For any lab device that contains Stefanini proprietary information, group account passwords must be changed within three (3) days following a change in group membership.
- No lab shall provide production services. Production services are defined as ongoing and shared business critical services that generate revenue streams or provide customer capabilities within or outside of Stefanini. These must be managed by the Support and Infrastructure Department.

3.2. General Configuration Guidelines

- All traffic between the corporate production and the lab network must go through a Stefanini maintained firewall or other device. Lab network devices (including wireless) must not cross-connect the lab and production networks.
- Original firewall configurations and any changes must be reviewed and approved by the Information Security Management Team. The Information Security Management Team may require security improvements as needed.
- Labs are prohibited from engaging in port scanning, network auto-discovery, traffic spamming/flooding, and other similar activities that negatively impact the corporate network and/or non-Stefanini networks. These activities must be restricted within the lab.
- Traffic between production networks and lab networks, as well as traffic between separate lab networks, is permitted based on business needs and as long as the traffic does not negatively impact other networks. Labs must not advertise network services that may compromise production network services or put lab confidential information at risk.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 533

- The Information Security Management Team reserves the right to audit all lab-related data and administration processes at any time, including but not limited to, inbound and outbound packets, firewalls and network peripherals.
- Lab owned gateway devices are required to comply with all Stefanini product security advisories and must authenticate against the Corporate Authentication servers.
- The enable password for all lab owned gateway devices must be different from all other equipment passwords in the lab. The password must be in accordance with *ISMS-043 Policy, Account and Password*. The password will only be provided to those who are authorized to administer the lab network.
- In labs where non-Stefanini personnel have physical access (e.g., training labs), direct connectivity to the corporate production network is not allowed. Additionally, no Stefanini confidential information can reside on any computer equipment in these labs. Connectivity for authorized personnel from these labs can be allowed to the corporate production network only if authenticated against the Corporate Authentication servers, temporary access lists (lock and key), SSH, client VPNs, or similar technology approved by the Information Security Management Team.
- All lab external connection requests must be reviewed and approved by the Information Security Management Team. Analog or ISDN lines must be configured to only accept trusted call numbers. Strong passwords must be used for authentication.
- All labs networks with external connections must not be connected to Stefanini corporate production network or any other internal network directly or via a wireless connection, or via any other form of computing equipment. An exception from the Information Security Management Team is required where air-gapping is not possible (e.g., Partner Connections to third party networks).

4. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Control for record protection	Retention time
Technology Lab Documentation	ICT Shared Drives; Request Ticketing System	N/A	Inherent System Controls	Records are stored for the life of the system plus 1 year.

5. Document management

The owner of this document is the Top Management Representative, who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria must be considered:

- number of Incidents related to a security breach within a technology lab

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 534

- number of Incidents related to production compromise as a result of technology lab activity

A current version of this document is available to all staff and under version control on the corporate document control system.

6. Appendices

- Not applicable.

7. Change history

Date	Version	Created by	Description of change
09-JUN-2014	1.0	Matthew Engler	Document creation

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 535

WIRELESS / ANALOG COMMUNICATION POLICY

Information Security Management System



Code:	ISMS-060NH
Version:	2.0
Date of version:	24-SEP-2014
Created by:	Matthew Engler
Approved by:	Stéphane Olmanst
Confidentiality level:	Internal Use

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 536

Table of contents

1. PURPOSE, SCOPE AND USERS 3
1.1. WIRELESS COMMUNICATIONS 3
1.2. ANALOG/ISDN LINES 3
2. REFERENCE DOCUMENTS 3
3. DESCRIPTION 4
3.1. WIRELESS COMMUNICATION 4
3.1.1. Wireless Communication Network Components 4
3.1.2. End User Wireless Communication Devices 4
3.2. ANALOG & ISDN LINES 4
3.2.1. Facsimile Machines 4
3.2.2. Computer-to-Analog Line Connections 5
4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 5
5. DOCUMENT MANAGEMENT 5
6. APPENDICES 5
6.1. WIRELESS INTERNET SERVICE ACCESS DISCLAIMER 5
7. CHANGE HISTORY 6

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 537

1. Purpose, scope and users

This policy provides the acceptable use and approved design and procedures for Wireless network and Analog/ISDN lines.

1.1. Wireless Communications

The policy prohibits access to Stefanini networks via unsecured wireless communication mechanisms. Only wireless systems that meet the criteria of this policy or have been granted an exception by the Information Security Team are approved for connectivity to Stefanini's networks. This policy establishes an authorized method for controlling mobile computing and storage devices that contain or access information resources at Stefanini.

This policy covers all wireless data communication devices (including mobile computing devices) connected to any of Northern Hemisphere Stefanini's internal networks. This includes any form of wireless communication device capable of transmitting packet data. Mobile computing devices includes either personally owned or Stefanini-owned, that may connect to or access the information systems at Stefanini. Wireless devices and/or networks without any connectivity to Stefanini's networks do not fall under the purview of this policy.

1.2. Analog/ISDN lines

For Analog & ISDN Lines, the policy covers two distinct uses of analog/ISDN lines: lines that are to be connected for the sole purpose of fax sending and receiving, and lines that are to be connected to computers.

This policy covers only those lines that are to be connected to a point inside a Northern Hemisphere Stefanini facility or testing site. It does not pertain to ISDN/phone lines that are connected into employee homes, PBX desktop phones, and those lines used by Telecom for emergency and non-corporate information purposes.

The policy is used by Stefanini Employees, sub-contractors, consultants, business associates, and other workers at Stefanini, including all personnel affiliated with third parties and subsidiaries on the Stefanini infrastructure (collectively "User(s)").

2. Reference documents

Documents associated or linked are listed below:

- ISO/IEC 27001 standard, A.13.1.1, A.13.1.2, A.13.2.1
- ISMS-001 Policy, Information Security
- ISMS-027 Policy, Information Transfer
- ISMS-028 Policy, Information Classification and Handling

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 538

3. Description

3.1. Wireless Communication

3.1.1. Wireless Communication Network Components

- All wireless Access Points / Base Stations connected to the corporate network must be registered and approved by the Information Security Team. These Access Points / Base Stations are subject to periodic penetration tests and audits. All wireless Network Interface Cards (i.e., PC cards) used in corporate laptop or desktop computers must be registered with the Information Security Team Office.
- All wireless LAN access must use corporate-approved vendor products and security configurations.

3.1.2. End User Wireless Communication Devices

- All mobile computing devices containing or accessing the information resources at Stefanini must be approved prior to connecting to the information systems at Stefanini. This pertains to all devices connecting to the network at Stefanini, regardless of ownership.
- All implementations must support a hardware address (i.e. a MAC address) that can be registered and tracked.
- Mobile computing devices may only be connected to a specified segment of the wireless network, controlling access to and from Stefanini resources.
- Technical personnel and users, which include employees, consultants, vendors, contractors, and students, shall have knowledge of, and adhere to the *Acceptable Use Policy*.
- Use of Stefanini wireless networks is subject to the *Wireless internet Access Service Disclaimer*.

3.2. Analog & ISDN Lines

3.2.1. Facsimile Machines

As a rule, the following applies to requests for fax and analog lines:

- No fax lines will be installed for personal use.
- No analog lines will be placed in a personal cubicle without expressed consent from the Information Security Team Office.

Exceptions for the above policy on analog-as-fax lines will be delivered on a case-by-case basis after reviewing the business need with respect to the level of sensitivity and security posture of the request.

Use of an analog/ISDN fax line is conditional upon the requester's full compliance with the requirements listed below. These requirements are the responsibility of the authorized user to enforce at all times:

- The fax line is used solely as specified in the request.
- Only persons authorized to use the line have access to it.
- When in use, the computer is to be physically disconnected from Stefanini's internal network.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 539

- The line will be used solely for Stefanini business and not for personal reasons.

3.2.2. Computer-to-Analog Line Connections

The general policy is that requests for computers or other intelligent devices to be connected with analog or ISDN lines from within Stefanini will not be approved for security reasons. Analog and ISDN lines represent a significant security threat to Stefanini.

External parties include various service providers, companies for hardware and software maintenance, companies handling transactions or data processing, clients, etc.

4. Managing records kept on the basis of this document

- Not applicable

5. Document management

The owner of this document is the Infrastructure and Support Departments, who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria must be considered:

- number of incidents related to misuse of wireless

A current version of this document is available to all staff and under version control on the corporate document control system.

6. Appendices

6.1. Wireless Internet Service Access Disclaimer

Wireless Internet Access Service provided “AS IS”. This Service provides access to the Internet on an “as is” basis with all the risks inherent in such access. The providers of the Service and Stefanini make no warranty that the Service, or that any information, software, or other material accessible on the Service, is free of viruses, worms, Trojan horses or other harmful components. By connecting, the user acknowledges and accepts the risks associated with public access to the Internet and public use of an unsecured wireless network.

Wireless Internet Access Service provided “AS AVAILABLE”. The Service is provided on an “as available” basis without warranties of any kind, either expressed or implied, that the Service will be uninterrupted or error-free, including but not limited to vagaries of weather, disruption of Service, acts of God, warranties of title, no infringement, NOR IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. No advice or information given by Stefanini providers, affiliates, or contractors of the Service or their respective employees shall create such a warranty.

No information you consider confidential should be transmitted via this network. By using this network, you agree to be solely responsible for the content of all information you disseminate. Users should be aware that there are security, privacy and confidentiality risks inherent in wireless communications and associated technology and Stefanini does not make any assurances or warranties relating to such risks. By using Wireless Internet Access, user agrees to indemnify and hold harmless the providers of the Service, including affiliates, agents, and contractors thereof, from any claim, liability, loss, damage, cost, or expense (including

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 540

without limitation reasonable attorney's fees) that result in any way from the user's use of, or inability to use, the Service, or to access the Internet or any part thereof, or user's reliance on or use of information, services or merchandise provided on or through the Service and/or any materials downloaded or uploaded through the Service, or that result from mistakes, omissions, interruptions, deletion of files, errors, defects, delays in operation, or transmission , or any failure of performance, any actions taken by you in connection with your use of the Service, or any violation of any third party's rights or a violation of law or regulation.

We reserve the right to deny or restrict access to any user who abuses the network, such as excessive bandwidth consumption or using the network for any type of activity or purpose deemed by Stefanini to be unlawful, harassing, abusive, criminal or fraudulent.

We also reserve the right to monitor, intercept and disclose any transmissions over or using our facilities, and to provide user information, or use records, and other related information under certain circumstances(for example, in response to lawful process, orders, subpoenas, or warrants, or to protect our rights, users or property) to appropriate authorities.

It is our policy to respond to notices of alleged infringement that comply with the Digital Millennium Copyright Act.

By using the Wi-Fi internet service provided by Stefanini you are agreeing to the disclaimer set forth above.

7. Change history

Date	Version	Created by	Description of change
13-FEB-2009	1.0	Matthew Engler	Document creation
24-SEP-2014	2.0	Matthew Engler	Updated to revised document design/numbering

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 541

REMOTE ACCESS POLICY

Information Security Management System



Code:	ISMS-061NH
Version:	2.0
Date of version:	24-SEP-2014
Created by:	Matthew Engler
Approved by:	Stéphane Olmanst
Confidentiality level:	Internal Use

Table of contents

1 PURPOSE, SCOPE AND USERS 3

1.1 REMOTE ACCESS POLICY 3

1.2 REMOTE VPN CONNECTIVITY STANDARD 3

2 REFERENCE DOCUMENTS 3

3 DESCRIPTION 4

3.1 REMOTE ACCESS POLICY 4

3.2 REMOTE VPN CONNECTIVITY STANDARD 4

4 MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 5

5 DOCUMENT MANAGEMENT 5

6 APPENDICES 6

7 CHANGE HISTORY 6

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 543

1 Purpose, scope and users

In order to allow Stefanini users the ability to access network resources from remote locations, Stefanini ICT makes systems and applications remotely available. This Policy defines the implementation requirements for protection of Stefanini ICT networks, systems, and information from the risks inherent in remote access without significantly impairing the quality of service to the remote user.

1.1 Remote Access Policy

This policy provides the mandatory minimum requirements to reduce risks to Stefanini ICT systems and data while enabling Stefanini staff to continue to remotely access ICT systems for official purposes. Specifically, this policy provides the basis for when two-factor authentication is required to access a Stefanini resource.

All equipment or devices deployed for remote access and/or operated by Stefanini (including hosts, routers, switches, etc.) and/or registered in any Domain Name System (DNS) domain owned by Stefanini must follow this policy.

This policy also covers any host device outsourced or hosted at external/third-party service providers, if that equipment resides in the "techteam.com" domain or appears to be owned by Stefanini.

This policy does not apply to systems that may require two-factor authentication for technological reasons, regardless of the system content

1.2 Remote VPN Connectivity Standard

The Remote VPN Connectivity Standard is intended to provide guidelines for Remote Access IPSec or Web-based Virtual Private Network (VPN) connections to the Stefanini corporate network.

This standard applies to all Stefanini Employees, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing VPNs to access the Stefanini network. This standard applies to implementations of VPN that are directed through an IPSec Concentrator.

2 Reference documents

Documents associated or linked are listed below:

- ISO/IEC 27001 standard, A.13.1.1, A.13.1.2, A.13.2.1
- ISMS-001 Policy, Information Security
- ISMS-027 Policy, Information Transfer
- ISMS-028 Policy, Information Classification and Handling

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 544

3 Description

3.1 Remote Access Policy

- Remote access systems must adhere to *ISMS-051, Server/System Security Policy*, and the *Remote VPN Connectivity Standard*, where applicable.
- Type Category Level: Stefanini categorizes remote access into three system types according to the risk of harm inherent in remote access and the sensitivity of the information accessed (See Information Classification and Handling Policy).
    - Type 1: Type 1 represents Low risk because the systems accessed are between the outermost Stefanini network perimeter device and inner local networks (i.e. DMZ). It is intended for access to Stefanini ICT services through the Internet. Information / data contained within this type is Public or Public / Confidential, where Confidential data represents low security risks relative to confidentiality, integrity and availability.
    - Type 2: Type 2 represents Moderate risk because basic user privileges are allowed to access systems processing or storing non-Restricted information internal to the Stefanini infrastructure environment. It is intended for access to internal Stefanini systems (i.e., inside the outermost Stefanini firewalls or perimeter gateway). This category includes users who authenticate to a Stefanini gateway (e.g. eVPN.techteam.com, reverse proxy) and are granted only partial access to the relevant network. Information / data contained within this type is Confidential, where Confidential data represents moderate security risks relative to confidentiality, integrity and availability. Computers used for this type of authenticated internal network access must be configured and maintained in a secure manner.
    - Type 3: Type 3 represents high risk because users are allowed to access systems processing or storing Confidential / Restricted information that is internal to the Stefanini infrastructure environment. This includes direct access to financial-related systems and administrative access to HR-related systems. It is also intended for administrative access to a Stefanini computer, database, or ICT resource on the internal network (e.g., using Cisco VPN Client). This category is usually used for obtaining remote administrator control but it also includes user level control when unrestricted user level access to the underlying operating system is obtained. Remote computers used for “remote control” access must be configured and maintained in a secure manner according to Stefanini’s Information Security Management System.
- Type 1 systems may allow access via one-factor authentication. Type 2 systems may allow access via one-factor authentication however, two-factor is preferred. Type 3 systems require two-factor authentication.

3.2 Remote VPN Connectivity Standard

Approved Stefanini Employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPNs, which are a "user managed" service. This means that the user is responsible for selecting

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 545

an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees.

Additionally,

- It is the responsibility of Stefanini Employees with Remote VPN privileges to ensure that unauthorized users are not allowed access to Stefanini internal networks.
- Remote VPN use is to be controlled using either a one-time password authentication (For Financial Data Access) such as a token device or individual login credentials.
- When actively connected to the corporate network, Remote VPNs will force all traffic to and from the PC over the Remote VPN tunnel; all other traffic will be dropped.
- Dual (split) tunneling is NOT permitted; only one network connection is allowed.
- Remote VPN gateways will be set up and managed by Stefanini's Global WAN Groups.
- All computers connected to Stefanini internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard (contact the Global Information Security Office for complete details); this includes personal computers.
- Remote VPN users will be automatically disconnected from Stefanini's network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
- The Remote VPN connection devices are limited to an absolute connection time of 24 hours.
- Users of computers that are not Stefanini-owned equipment must configure the equipment to comply with Stefanini's VPN and Network policies.
- Only Global Information Security Office-approved VPN clients may be used.
- By using Remote VPN technology with personal equipment, users must understand that their machines are a de facto extension of Stefanini's network, and as such are subject to the same rules and regulations that apply to Stefanini-owned equipment, i.e., their machines must be configured to comply with Stefanini Global Information Security Policies.

4 Managing records kept on the basis of this document

- Not applicable

5 Document management

The owner of this document is the Infrastructure and Support Departments, who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria must be considered:

- number of incidents related to misuse of VPN Connections

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 546

- number of requests for externally available systems

A current version of this document is available to all staff and under version control on the corporate document control system.

6 Appendices

- N/A

7 Change history

Date	Version	Created by	Description of change
13-FEB-2009	1.0	Matthew Engler	Document creation
24-SEP-2014	2.0	Matthew Engler	Updated to revised document design/numbering

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 547

AUTOMATICALLY FORWARDED EMAIL POLICY

Information Security Management System



Code:	ISMS-062NH
Version:	2.0
Date of version:	24-SEP-2014
Created by:	Matthew Engler
Approved by:	Stéphane Olmanst
Confidentiality level:	Internal Use

Table of contents

1. PURPOSE, SCOPE AND USERS 3
2. REFERENCE DOCUMENTS 3
3. DESCRIPTION 3
4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 3
5. DOCUMENT MANAGEMENT 3
6. APPENDICES 3
7. CHANGE HISTORY 4

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 549

1. Purpose, scope and users

The *Automatically Forwarded Email Policy* is intended to prevent the unauthorized or inadvertent disclosure of confidential or restricted company information.

This policy covers automatic email forwarding, and thereby the potentially inadvertent transmission of confidential or restricted information by all Stefanini Employees, vendors, and agents operating on behalf of Stefanini.

2. Reference documents

Documents associated or linked are listed below:

- ISO/IEC 27001 standard, A.8.2.1, A.13.2.1
- ISMS-001 Policy, Information Security
- ISMS-027 Policy, Information Transfer
- ISMS-028 Policy, Information Classification and Handling

3. Description

Stefanini Employees must exercise utmost caution when sending any email from inside Stefanini to an outside network. Unless approved by a manager through the Information Security Management Team, Stefanini email will not be automatically forwarded to an external destination. If required, emails will be allowed to automatically forward to a Stefanini customer email account, assuming Stefanini has a contract/non-disclosure in place with the customer.

4. Managing records kept on the basis of this document

- Not applicable

5. Document management

The owner of this document is the Infrastructure and Support Departments, who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria must be considered:

- number of incidents related to unauthorized disclosure

A current version of this document is available to all staff and under version control on the corporate document control system.

6. Appendices

- N/A

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 550

7. Change history

Date	Version	Created by	Description of change
13-FEB-2009	1.0	Matthew Engler	Document creation
24-SEP-2014	2.0	Matthew Engler	Updated to revised document design/numbering

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 551

PERSONAL COMMUNICATION DEVICE AND VOICEMAIL STANDARD

Information Security Management System



Code:	ISMS-063NH
Version:	2.0
Date of version:	24-SEP-2014
Created by:	Matthew Engler
Approved by:	Stéphane Olmanst
Confidentiality level:	Internal Use

Table of contents

1 PURPOSE, SCOPE AND USERS 3
2 REFERENCE DOCUMENTS 3
3 DESCRIPTION 3
3.1 GENERAL 3
3.2 BLUETOOTH 4
3.3 VOICEMAIL 4
3.4 LOSS AND THEFT 4
3.5 PERSONAL USE 4
3.6 PCD SAFETY 4
4 MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 4
5 DOCUMENT MANAGEMENT 4
6 APPENDICES 5
7 CHANGE HISTORY 5

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 553

1 Purpose, scope and users

The *Personal Communication Devices and Voicemail Standard* is intended to describe Stefanini's requirements for Personal Communication Devices and Voicemail.

This standard applies to any use of Personal Communication Devices (PCDs) and Stefanini Voicemail issued by Stefanini or used for Stefanini business. For the purpose of this policy, PCDs are defined to include handheld wireless devices, cellular telephones (including Blackberry Devices and PDAs), laptop wireless cards, tablets (e.g. iPad) and pagers.

2 Reference documents

Documents associated or linked are listed below:

- ISO/IEC 27001 standard, A.6.2.1, A.9.4.2, A.11.2.6, A.11.2.8
- ISMS-001 Policy, Information Security
- ISMS-029 Policy, Bring Your Own Device - BYOD
- ISMS-047 Policy, Mobile Device and Teleworking

3 Description

3.1 General

Personal Communication Devices (PCDs) will be issued only to Stefanini Employees with duties that require them to be in immediate and frequent contact when they are away from their normal work locations. Effective distribution of the various technological devices must be limited to persons for whom the productivity gained is appropriate in relation to the costs incurred.

For any PCD which connects to the Stefanini infrastructure for purposes of receiving Stefanini email or performing business related transactions, the following minimum settings must be adhered to:

- Numeric PIN Protected
    - 4-digit PIN – Required
    - 8-digit PIN – Recommended
- Simple PINs disallowed
- Automatic lock after 15 minutes
- Grace period of 2 minutes
- Automatic wipe/permanent lock after ten wrong tries; Stefanini can remote wipe device (if applicable)
- No direct push when roaming

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 554

3.2 Bluetooth

Hands-free enabling devices, such as the Bluetooth, may be issued to authorized Stefanini Employees who have received approval. Care must be taken to avoid being recorded when peering Bluetooth adapters, Bluetooth 2.0 Class 1 devices have a range of 330 feet. When Bluetooth devices are not being used it is imperative that Bluetooth is disabled to prevent connectivity from other devices. When possible, do not use the default password from the vendor for peering your Bluetooth devices.

3.3 Voicemail

Voicemail boxes may be issued to Stefanini Employees who require a method for others to leave messages when they are not available. Voicemail boxes must be protected by a PIN which must never be the same as any of the consecutive digits of the telephone number of the voicemail box.

3.4 Loss and Theft

Files (excluding email) containing confidential or restricted data may not be stored in PCDs unless protected by approved encryption. Confidential or restricted data shall never be stored on a personal PCD. Charges for repair due to misuse of equipment or misuse of services may be the responsibility of the Stefanini Employee, as determined on a case-by-case basis. The cost of any item beyond the standard authorized equipment is also the responsibility of the Stefanini Employee. Lost or stolen equipment must immediately be reported by contacting the Stefanini Service Desk.

3.5 Personal Use

PCDs and voicemail are issued for Stefanini business. Personal use must be limited to minimal and incidental use.

3.6 PCD Safety

Conducting telephone calls or utilizing PCDs while driving can be a safety hazard. Drivers should use PCDs while parked or out of the vehicle. If Stefanini Employees must use a PCD while driving, Stefanini requires the use of hands-free enabling devices.

4 Managing records kept on the basis of this document

- Not applicable

5 Document management

The owner of this document is the Infrastructure and Support Departments, who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria must be considered:

- number of incidents related to unauthorized disclosure
- number of incidents related to lost devices

A current version of this document is available to all staff and under version control on the corporate document control system.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 555

6 Appendices

- N/A

7 Change history

Date	Version	Created by	Description of change
13-FEB-2009	1.0	Matthew Engler	Document creation
24-SEP-2014	2.0	Matthew Engler	Updated to revised document design/numbering

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 556

CREDIT CARD DATA HANDLING STANDARD

Information Security Management System



Code:	ISMS-064NH
Version:	2.0
Date of version:	24-SEP-2014
Created by:	Matthew Engler
Approved by:	Stéphane Olmanst
Confidentiality level:	Internal Use

Table of contents

1. PURPOSE, SCOPE AND USERS 3
2. REFERENCE DOCUMENTS 3
3. DESCRIPTION 3
4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 4
5. DOCUMENT MANAGEMENT 4
6. APPENDICES 4
7. CHANGE HISTORY 4

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 558

1. Purpose, scope and users

The *Credit Card Data Handling Standard* is intended to help Stefanini maintain compliance regarding the handling of Credit Card data with Payment Card Industry (PCI) standards. Failure to comply with these regulations not only subjects our customers to unnecessary risk but also exposes Stefanini to significant fines and potentially the loss of credit card handling privileges.

This standard applies to Stefanini Employees, sub-contractors, consultants, business associates, and other workers at Stefanini including all personnel affiliated with third parties and subsidiaries having access to a Stefanini Data (collectively "User(s)").

This policy applies to any Stefanini project, delivery group or business unit where a payment card's primary account number (PAN) is stored, processed or transmitted.

2. Reference documents

Documents associated or linked are listed below:

- ISO/IEC 27001 standard, A.8.2.1, A.18.1.1, A.18.1.4
- ISMS-001 Policy, Information Security
- ISMS-028 Policy, Information Classification and Handling

3. Description

Credit Cards and Credit Card data must be protected according to the following standard:

- The full credit card number must only be available to those few individuals whose job requires access, or entities that have a business need to view the full credit card number.
- Payment processing is only performed via a virtual terminal accessed by an Internet-connected web browser.
- The payment processing virtual terminal solution is provided and hosted by a PCI-DSS validated third-party service provider.
- Firewall or network segmentation is in place to isolate computers used to access the virtual terminal solution.
- Computers do NOT have installed any software that causes cardholder data to be stored (e.g. software for batch processing or store-and-forward).
- Computers do NOT have installed any attached hardware devices that are used to capture or store cardholder data (e.g., no card readers attached).
- Payment transactions are not received or transmitted electronically through any other channels (e.g. via an internal network or the Internet).
- Credit card data is classified as Restricted data and must be protected in accordance with the ISMS-028 Information Classification and Handling Policy.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 559

- Paper reports or paper copies of receipts are disposed of when no longer required for legal, regulatory, or business reasons. This disposal must occur in a manner consistent with the destruction of Restricted data.
- Cardholder data is NOT stored in electronic format.

4. Managing records kept on the basis of this document

- Not applicable

5. Document management

The owner of this document is the Infrastructure and Support Departments, who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria must be considered:

- number of incidents related to disclosure of Credit Card data
- number of projects performing such work increases

A current version of this document is available to all staff and under version control on the corporate document control system.

6. Appendices

- Not applicable

7. Change history

Date	Version	Created by	Description of change
13-FEB-2009	1.0	Matthew Engler	Document creation
24-SEP-2014	2.0	Matthew Engler	Updated to revised document design/numbering

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 560

TECHNICAL COMPLIANCE REVIEW POLICY

Information Security Management System



Code:	ISMS-065NH
Version:	2.0
Date of version:	24-SEP-2014
Created by:	Matthew Engler
Approved by:	Stéphane Olmanst
Confidentiality level:	Internal Use

Table of contents

1. PURPOSE, SCOPE AND USERS 3
1.1. SECURITY SCANNING POLICY 3
1.2. SECURITY SCANNING STANDARDS 3
2. REFERENCE DOCUMENTS 3
3. DESCRIPTION 3
3.1. GENERAL REQUIREMENTS 3
3.2. SECURITY SCANNING POLICY 4
3.3. SECURITY SCANNING STANDARDS 4
3.3.1. Initial System Vulnerability Scan 4
3.3.2. External Vulnerability Scans 5
4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 5
5. DOCUMENT MANAGEMENT 5
6. APPENDICES 6
7. CHANGE HISTORY 6

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 562

1. Purpose, scope and users

The *Technical Compliance Review Policy* covers those activities taken to ensure the compliance of systems with Stefanini's technical security requirements and current best practices. The policy includes general requirements and information specific to security scanning.

1.1. Security Scanning Policy

The *Security Scanning Policy* is designed to help provide feedback on the security program's effectiveness. Regularly scheduled, proactive scanning of the devices and applications attached to the network is a best practice for managing a dynamic computing environment and necessary to locate and eliminate possible vulnerabilities.

This policy applies to all systems attached to the Stefanini network which may be subject to security vulnerability scans.

1.2. Security Scanning Standards

The Security Scanning Standards are designed to provide a baseline for performing security scans of the Stefanini infrastructure. Regularly scheduled, proactive scanning of the devices and applications attached to the network is a best practice for managing a dynamic computing environment and necessary to locate and eliminate possible vulnerabilities.

2. Reference documents

Documents associated or linked are listed below:

- ISO/IEC 27001 standard, A.18.2.1, A.18.2.3
- ISMS-001 Policy, Information Security
- ISMS-051 Policy, Server / System Security Policy

3. Description

3.1. General Requirements

- Security scans will be performed according the policy / standard documented.
- Penetration tests may be performed. If performed, a qualified third party should be utilized with a defined scope and plan.
- Any technical compliance review will be performed to minimize impact to the infrastructure.
- Where possible, a third party vendor should be utilized to provide an independent review.
- Stefanini will use a third party to maintain a baseline of externally exposed IPs and current port status. Changes in port status must be escalated to the Information Security Team. Escalations will occur through an Incident in Stefanini Service Desk.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 563

3.2. Security Scanning Policy

Stefanini will define and maintain a multipoint security scanning program which will fulfil regulatory requirements, demonstrate due diligence toward protecting our customers and suppliers and enable the identification and elimination of vulnerabilities.

The following conditions must be observed as part of the policy:

- **Responsibility** - Security scans will only be executed under the coordination of the Global Information Security Office or ICT Support Groups.
- **Negligible Disruption to Business** - Reasonable precautions will be taken to ensure that business operations are not negatively impacted by the scanning process.
- **Change Order** - Where any potential impact may be observed, a change order will be created in the Stefanini Service Desk to document the scanning activity. The change order will describe any potential risks, specify the time period during which the scan will take place, provide a plan for recovery from any negative impact and require approval of all significant stake holders before the scan can be executed.
- **Denial of Service Scans** - Because Denial-of-Service scans are an attempt to disrupt service and may actually do so, no such scans will be performed without first consulting and coordinating the effort with the owners, managers and administrators of all potentially impacted systems.
- **Scanning Requirements**
    - Initial server vulnerability scans prior to production deployment in the environment
    - Internal vulnerability scans as required by current risks
    - External vulnerability scans at least quarterly and after major changes or upgrades (must be completed by ASV certified vendors)

3.3. Security Scanning Standards

3.3.1. Initial System Vulnerability Scan

Stefanini utilizes a professional, updated solution to conduct scans of any Stefanini server being deployed to infrastructure. The required procedures for these scans are:

- The server administration team will build the server per the requested specifications.
- The application team will install and configure the required applications to meet the server's purpose.
- The server administration team or information security team will perform the vulnerability scan.
- The server administration team coordinates remediation of any vulnerabilities identified by the scans prior to the device being release for production.
    - Critical – Must be remediated prior to deployment (or external connectivity).
    - High – Should be remediated prior to deployment (or external connectivity).

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 564

- All others will be reviewed.

3.3.2. *External Vulnerability Scans*

Stefanini contracts with a PCI approved scanning vendor (ASV) to conduct quarterly scans of all Stefanini web sites and IT infrastructures with internet facing IP addresses. The required procedures for these scans are:

- The ASV is provided with a complete listing of IP addresses or IP address ranges to be scanned.
- IDS devices are configured so that they will not interfere with the ASV's activities.
- Based on the provided addresses the ASV probes to determine which IP addresses and services are active.
- The ASV scans all active devices found including:
  - Firewalls
  - External Routers
  - Web Servers
  - Application servers
  - Domain Named Servers (DNSs).
  - Mail Servers
  - Virtual Hosts
- The Stefanini Information Security Team coordinates remediation of any vulnerabilities identified by the scans through a Vulnerability Management Procedure.

4. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
Stefanini Service Desk Incident	Stefanini Service Desk	Information Security Manager	Only authorized personnel have access.	Life of the affected system.

5. Document management

The owner of this document is the Infrastructure and Support Departments, who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria must be considered:

- number of vulnerabilities identified
- Incidents caused by scanning activity

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 565

A current version of this document is available to all staff and under version control on the corporate document control system.

6. Appendices

- Not applicable

7. Change history

Date	Version	Created by	Description of change
13-FEB-2009	1.0	Matthew Engler	Document creation
24-SEP-2014	2.0	Matthew Engler	Updated to revised document design/numbering

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 566

stefanini
POWERING YOUR BUSINESS

SECURE DEVELOPMENT SECURITY REQUIREMENTS

Information Security Management System



Code:	ISMS-066NH
Version:	1.0
Date of version:	24-SEP-2014
Created by:	Matthew Engler
Approved by:	Stéphane Olmanst
Confidentiality level:	Internal Use

Table of contents

1. PURPOSE, SCOPE AND USERS 3
1.1. Application Development Standards 3
1.2. Database Password Standards 3
1.3. Wildcard SSL Certificate Standard 3
2. REFERENCE DOCUMENTS 3
3. DESCRIPTION 4
3.1. General Requirements 4
3.2. Application Development Standards 4
3.3. Database Password Standards 4
3.3.1. General 4
3.3.2. Specific Requirements 4
Storage of Data Base User Names and Passwords 4
Retrieval of Database User Names and Passwords 5
Access to Database User Names and Passwords 5
3.4. Wildcard SSL Certificate Standard 5
4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 5
5. DOCUMENT MANAGEMENT 6
6. APPENDICES 6
7. CHANGE HISTORY 6

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 568

1. Purpose, scope and users

The *Secure Development Security Requirements* covers how environments and deployments in the Stefanini infrastructure will be designed to ensure a secure design and deployment. It is designed to also meet the requirements of section 3.1.5 of *ISMS-046, Secure Development Policy*. The security requirements include general requirements and information specific to Application Development, Database Passwords and Wildcard SSL Certificates.

1.1. Application Development Standards

The Application Development Standards states basic requirements for developing an application or deploying a pre-packaged application for which configuration changes can be made.

1.2. Database Password Standards

The *Database Password Standard* states the requirements for securely storing and retrieving database usernames and passwords (i.e., database credentials) for use by a program that will access a database running on one of Stefanini's networks.

Computer programs running on Stefanini's networks often require the use of one of the many internal database servers. In order to access one of these databases, a program must authenticate to the database by presenting acceptable credentials. The database privileges that the credentials are meant to restrict can be compromised when the credentials are improperly stored.

1.3. Wildcard SSL Certificate Standard

A *Wildcard SSL Certificate Standard* helps enable SSL encryption on multiple sub-domains using a single certificate as long as the domains are controlled by the same organization and share the same second-level domain name.

Wildcard SSL Certificates pose a few security / data risks. If one server or sub-domain is compromised, all sub-domains may be compromised. Also, if the wildcard certificate needs to be revoked, all sub-domains will need a new certificate. Wildcard SSL Certificates may only be used per the defined policy.

This policy applies to server equipment owned and/or operated by Stefanini and to servers registered under any Stefanini-owned network domain where communication must be secured via an SSL certificate.

2. Reference documents

Documents associated or linked are listed below:

- ISO/IEC 27001 standard, A.14.1
- ISMS-001 Policy, Information Security
- ISMS-051 Policy, Server / System Security Policy
- ISMS-061NH Policy, Remote Access.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 569

3. Description

3.1. General Requirements

- Systems and Servers will be deployed in accordance with *ISMS-051 Policy, Server / System Security Policy*.
- If remote access is required, it will be deployed in accordance with *ISMS-061NH Policy, Remote Access.*
- Any issues discovered through a technical compliance review will require remediation or mitigation, depending upon the issue.

3.2. Application Development Standards

Application developers must ensure their programs contain the following security precautions. Applications:

- Must support authentication of individual users, not groups.
- Must not store passwords in clear text or in any easily reversible form.
- Must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
- Must support TACACS+, RADIUS and/or X.509 with LDAP security retrieval, wherever possible.
- Should follow development standards best practices.

3.3. Database Password Standards

3.3.1. General

In order to maintain the security of Stefanini's internal databases, access by software programs must be granted only after authentication with credentials. The credentials used for this authentication must not reside in the main, executing body of the program's source code in clear text. Database credentials must not be stored in a location that can be accessed through a web server.

3.3.2. Specific Requirements

Storage of Data Base User Names and Passwords

- Database user names and passwords may be stored in a file separate from the executing body of the program's code. This file must not be world readable.
- Database credentials may reside on the database server. In this case, a hash number identifying the credentials may be stored in the executing body of the program's code.
- Database credentials may be stored as part of an authentication server (i.e., an entitlement directory), such as an LDAP server used for user authentication. Database authentication may occur on behalf of a program as part of the user authentication process at the authentication server. In this case, there is no need for programmatic use of database credentials.
- Database credentials may not reside in the documents tree of a web server.
- Pass through authentication (i.e., Oracle OPS$ authentication) must not allow access to the database based solely upon a remote user's authentication on the remote host.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 570

- Passwords or passphrases used to access a database must adhere to the Password Policy.

Retrieval of Database User Names and Passwords

- If stored in a file that is not source code, then database user names and passwords must be read from the file immediately prior to use. Immediately following database authentication, the memory containing the user name and password must be released or cleared.
- The scope into which you may store database credentials must be physically separated from the other areas of your code, e.g., the credentials must be in a separate source file. The file that contains the credentials must contain no other code but the credentials (i.e., the user name and password) and any functions, routines, or methods that will be used to access the credentials.
- For languages that execute from source code, the credentials' source file must not reside in the same browse able or executable file directory tree in which the executing body of code resides.

Access to Database User Names and Passwords

- Every program or every collection of programs implementing a single business function must have unique database credentials. Sharing of credentials between programs is not allowed.
- Database passwords used by programs are system-level passwords as defined by the Password & Passphrase Standard.
- Developer groups must have a process in place to ensure that database passwords are controlled and changed in accordance with the Password & Passphrase Standard. This process must include a method for restricting knowledge of database passwords to a need-to-know basis.

3.4. Wildcard SSL Certificate Standard

- A wildcard SSL certificate may only be used on sites of a non-critical nature (i.e. with lower required availability).
- A wildcard SSL certificate may only be used where the expected data transactions fall under either Public or Confidential classifications. Under no circumstances may it be used where the expected data transactions are a Restricted classification. If data classified as Restricted is found to be transmitted using a system protected by a wildcard SSL certificate, the system must be taken offline immediately until a unique certificate can be issued and applied.
- If a wildcard SSL certificate is found to be compromised, all systems which use that certificate must be taken offline immediately until a new certificate can be issued and applied.
- All systems / sites secured with a wildcard SSL certificate must be documented. This list must be maintained by the system owner and a copy provided to the Global Information Security group.
- A wildcard SSL certificate must be issued by an authorized Certificate Authority.
- A wildcard SSL certificate may not be used to secure a site / system intended for client use or which transmits primarily client data.

4. Managing records kept on the basis of this document

- Not applicable

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 571

5. Document management

The owner of this document is the Infrastructure and Support Departments, who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria must be considered:

- number of vulnerabilities identified
- Incidents caused by scanning activity

A current version of this document is available to all staff and under version control on the corporate document control system.

6. Appendices

- Not applicable

7. Change history

Date	Version	Created by	Description of change
24-SEP-2014	1.0	Matthew Engler	Document creation

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 572

PATCHING AND VULNERABILITY MANAGEMENT PROCEDURE

Information Security Management System



Code:	ISMS-067
Version:	2.0
Date of version:	26-AUG-2020
Updated by:	Matthew Engler
Approved by:	Washington Souza
Confidentiality level:	Internal Use

Table of contents

1. PURPOSE, SCOPE AND USERS 3

1.1. PURPOSE 3

1.2. SCOPE 3

1.3. USERS 3

2. REFERENCE DOCUMENTS 3

3.1 POLICY 3

3.1.1 SERVER INFRASTRUCTURE 3

3.1.2 NETWORK INFRASTRUCTURE 4

3.1.3 ENDPOINTS 5

3.2 PROCEDURE 5

3.2.1 SERVERS AND NETWORK DEVICES 5

3.2.2 QA, DEVELOPMENT 5

3.2.3 PRODUCTION 5

3.2.4 END-USERS COMPUTERS 5

3.2.5 ZERO-DAY AND EMERGENCY SECURITY PATCHING: 5

3.2.6 INSTALLATION AND VALIDATION 6

3.2.7 PATCH-COMPLIANCE REVIEW 6

3.2.8 EXCEPTIONS 7

3.3 RESPONSIBILITIES 7

4. VULNERABILITY MANAGEMENT POLICY & PROCEDURE 8

4.1. POLICY 8

4.2. PROCEDURES 8

4.2.1. NOTIFICATIONS OF VULNERABILITIES 8

4.2.2. VENDOR OR SPECIAL INTEREST GROUP NOTIFICATIONS 8

4.2.3. VULNERABILITY SCANS 9

4.2.4. PENETRATION TEST / OTHER TECHNICAL COMPLIANCE REVIEW 11

4.2.5. REMEDIATION 11

4.2.6. RESPONSIBILITIES 14

5. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 14

6. DOCUMENT MANAGEMENT 15

7. APPENDICES 15

8. CHANGE HISTORY 15

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 574

1. Purpose, scope and users

1.1. Purpose

Stefanini is committed to ensuring a secure computing environment and recognizes the need to prevent and manage IT vulnerabilities. A compromised computer threatens the integrity of the network and all computers connected to it. Patch and vulnerability management is a security practice designed to proactively prevent the exploitation of IT vulnerabilities that exist within an organization. Proactively managing vulnerabilities will reduce or eliminate the potential for exploitation and involve considerably less time and effort than responding after exploitation has occurred.

The purpose of this policy and procedure is to ensure that all Stefanini-owned devices are proactively managed and patched with appropriate security updates.

1.2. Scope

This process defines the steps that will be followed to maintain existing systems with known patches and to manage vulnerabilities discovered through technical compliance audits, security scans or external notifications of vulnerabilities.

1.3. Users

This process is used by the Information Security Team, ICT and Application teams to coordinate the remediation of discovered vulnerabilities.

2. Reference documents

Documents associated or linked tare listed below:

- ISO/IEC 27001 standard, A.12.5.1, A.12.6.1, A.14.2.2, A.18.2.3
- ISMS-001 Policy, Information Security
- ISMS-065NH Policy, Technical Compliance Review

3. Patch Management Policy & Procedure

3.1 Policy

3.1.1 Server Infrastructure

All servers managed by Stefanini ICT will be maintained with the latest security patches to their operating systems and key, common applications.

Each application owner is responsible for installed applications under their control. Application owners must ensure that their staff maintain knowledge of patch releases either through subscribing to the appropriate mailing list or by direct notification from the vendor.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 575

When a patch is announced, an authorized system administrator must enter a change order (CO) according to the change management policy. When the CO is entered, the category of CO must be determined. Patching performed during a normal maintenance window will be Standard or Normal as the impact dictates. Patches applied outside a normal maintenance window will be categorized as Emergency.

All critical operating system patches must be applied as soon as practically possible, but ***not longer than 72 hours*** after public release. All high patches must be applied as soon as practically possible, but ***not longer than forty five (45) calendar days*** after public release for any critical production server. All patches that are medium/high severity or for non-critical systems must be rolled out ***within ninety (90) calendar days***. Any low severity patches will be installed on a case-by-case basis. All patches should be tested on development systems before being rolled out to production, where possible.

In the case where patches cannot follow the aforementioned schedule, a Request must be documented explaining why the patch must be deferred. Permissible deferrals may include a lack of appropriate change windows within the appropriate timeframe or a conflict with other critical changes scheduled at that time. Any patches which are to be deferred longer than the scheduled timeframe must be approved by Security management. All deferred patches must be reviewed at least quarterly.

All patches for vendor maintained systems/applications that are labelled as high/critical and apply to security must also be patched **within ninety (90) days** of the approved release from the vendor. Any functional but non-critical patches may be installed on a case-by-case basis. Stefanini ICT / Application Owner are responsible for maintaining knowledge of these patches and ensuring that vendors comply with the policy.

A schedule for the monthly application of patches will be developed and published by application, ICT, and Change Management organizations.

Vulnerability scans will be performed on systems after each patch window to show that the patches were installed correctly.

3.1.2 Network Infrastructure

All network devices managed by Stefanini ICT will be maintained with the latest security patches to their operating systems and key, common applications.

When a patch is announced, an authorized system administrator must enter a change order (CO) according to the change management policy. When the CO is entered, the category of CO must be determined. Patching performed during a normal maintenance window will be Standard or Normal as the impact dictates. Patches applied outside a normal maintenance window will be categorized as Emergency.

All critical system patches must be applied as soon as practically possible, but ***not longer than 72 hours*** after public release. All high patches must be applied as soon as practically possible, but ***not longer than forty five (45) calendar days*** after public release for any critical systems. All patches that are medium/high severity or for non-critical systems must be rolled out ***within ninety (90) calendar days***. Any low severity patches will be installed on a case-by-case basis. All patches should be tested on development systems before being rolled out to production, where possible.

In the case where patches cannot follow the aforementioned schedule, a Request must be documented explaining why the patch must be deferred. Permissible deferrals may include a lack of appropriate change windows within the appropriate timeframe or a conflict with other critical changes scheduled at that time. Any patches which are to be deferred longer than the scheduled timeframe must be approved by Security management. All deferred patches must be reviewed at least quarterly.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 576

3.1.3 Endpoints

All Stefanini-owned Windows based endpoints are to have operating system and key application patches installed within ***14 days*** of release from the vendor. All critical operating system patches must be applied as soon as practically possible, but ***not longer than 72 hours*** after public release.

3.2 Procedure

3.2.1 Servers and network devices

1. Scan for available patches via WSUS, SCCM, or Vendor-supplied
2. Download necessary patches from a trusted source (as made available)
3. Create a change order one week before the maintenance date
4. Deploy patches
5. Verify services
6. Notify and report testing results

3.2.2 QA, Development

1. Scan for available patches
2. Download necessary patches from a trusted source (as made available)
3. Deploy patches
4. Verify services
5. Notify and report testing results

3.2.3 Production

1. Patches are initially approved, deployed, and applied in development (where available)
2. Create a change order one week before the maintenance date
3. The Customer Support team notifies the customer of maintenance
4. Deploy patches
5. Communicate extended outages to appropriate teams. If outage goes past window, Stefanini Service Desk must communicate it to the organization
6. Verify services

3.2.4 End-users computers

1. Scan for available patches
2. Download necessary patches from a trusted source (as made available)
3. Schedule deployment
4. Deploy patches

3.2.5 Zero-day and emergency security patching:

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 577

Note: The Security team will determine the risk and the relevance of the patch, as well as when the system should be patched.

1. Create a order before the maintenance date
2. Notify users
3. Deploy patches
4. Verify services
5. Notify and report testing results

3.2.6 Installation and Validation

A system reboot is required to successfully install most security patches. Until the reboot occurs, the computer remains vulnerable to attacks which the installed patch protects against. Stefanini ICT understands the impact an ill-timed reboot can have on user productivity. In order to provide the Stefanini community with as much flexibility as possible, security updates will be deployed using an "optional-mandatory" method.

The optional-mandatory method will allow users to install scheduled update at their convenience before a deadline occurs. Users will be provided **twenty-four (24) hours** to select the installation time of their choosing for deployed patches. After the deadline passes, updates will automatically install and may enforce reboots of the computer, as the updates require. It is strongly recommended that users install the updates as soon as possible to ensure that end points are protected and rebooting does not disrupt work. When updates are available, a notification will appear in the system tray. The message will continue to appear until the updates are installed and will appear more frequently as the deadline approaches.

3.2.7 Patch-Compliance Review

1. The ICT Risk Management team will generate and review patch management/compliance reports on at least a monthly basis from the company vulnerability management tools.
2. In reviewing the patch reports, The ICT Risk Management team will identify unpatched machines that connect to the company network. An Incident will be created in Stefanini Service Desk to track remediation.
3. ICT security, via 3rd party, will conduct an external vulnerability scan on at least a quarterly basis to identify known and potential vulnerabilities with the publicly facing system. Vulnerabilities will be brought to the attention of the system/application administrator(s) for mitigation.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 578

3.2.8 Exceptions

Systems or applications that cannot be patched to resolve a known vulnerability will have the justification documented by the device/application owner and the necessary compensating control(s) implemented:

- Justification:
  - No vendor patch available
  - Patch provided by vendor creates instability within the system; instability outweighs the risk.
- Compensating Controls
  - Network segmentation
  - Access Control Lists
  - Intrusion Prevention System

Systems that transmit or store protected data and cannot be patched to resolve a known vulnerability will be brought to the attention of the data owner (typically the ICT Risk Director, Vice President of Infrastructure, and the department Director) and the necessary compensating control(s) will be implemented.

3.3 Responsibilities

Role	Responsibility
Top Management Representative	Review and approve changes to the Patch Management Policy and Procedures
Information Security Team	Scan for patches (Vulnerability Management Program)
ICT / Application Team	Obtain patches for systems
ICT / Application Team	Notify teams (QA, DEV, pre-prod and production) of patching schedules (depending on environment)
ICT / Application Team	Apply patches
QA/Dev Engineer	Test services after patching
QA/Dev Engineer	Notify and report testing results
ICT / Application Team; Information Security Team	Remediate issues, as necessary

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 579

4. Vulnerability Management Policy & Procedure

4.1. Policy

All patches or configuration changes must be deployed to Stefanini owned or managed ICT systems per the timeframe stated in the Patching and Vulnerability Management Procedure.

The Information Security Team provides approved standard tools and methodologies for vulnerability assessments.

All ICT systems must be part of a patch management cycle as defined in the Patch Management Policy & Procedure section.

Application and system owners are responsible for the assessment and remediation of ICT systems under their management or supervision.

If a solution or remediation is not available to address a vulnerability, the Information Security Team must approve any compensating or other mitigating controls.

Application and system owners must have a written and auditable procedure addressing remediation steps.

4.2. Procedures

4.2.1. Notifications of Vulnerabilities

Vulnerabilities may come from a variety of sources. These include:

- Vendor or Special Interest Group notifications
- Security Incident
- Vulnerability Scans
- Penetration Tests
- Other types of Technical Compliance audits

4.2.2. Vendor or Special Interest Group Notifications

Stefanini may receive notification of a vulnerability from the vendor or through various special interest groups. These may require action be taken to reduce exposure or a patch may need to be applied. The Information Security Team will review incoming vulnerability notifications and work with the ICT / Application teams to understand exposure. If exposure is normal, a decision will be made with the asset owner to allow the vulnerability to be corrected during a normal maintenance cycle or an acceptance of the vulnerability.

If exposure is high, a decision will be made with the asset owner on whether to perform an Emergency correction, allow it to be corrected during a normal maintenance cycle or to accept the vulnerability.

If Emergency corrective actions are authorized, an Emergency Change Order will be placed in the Stefanini Service Desk system and will follow the Change Management Process.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 580

- Security Incident

Stefanini may receive notification of a vulnerability through a Security Incident. These may require action be taken to reduce exposure or a patch may need to be applied. The Information Security Team will review the Security Incident and work with the ICT / Application teams to understand exposure. If exposure is normal, a decision will be made with the asset owner to allow the vulnerability to be corrected during a normal maintenance cycle or an acceptance of the vulnerability.

If exposure is high, the Incident will be handled as part of an Incident Response. A decision will need to be made on whether to perform an Emergency correction, allow it to be corrected during a normal maintenance cycle or to accept the vulnerability. A decision from the asset owner will be sought, but the Information Security Team / ICT may take action without asset owner approval if exposure to the stability of the infrastructure is too high or the Security Incident presents a clear and present danger to Stefanini's Infrastructure.

A Stefanini Incident will be created (or exist) within the Stefanini Service Desk. If appropriate, an Emergency Change Order will be placed in the Stefanini Service Desk system and will follow the Change Management Process.

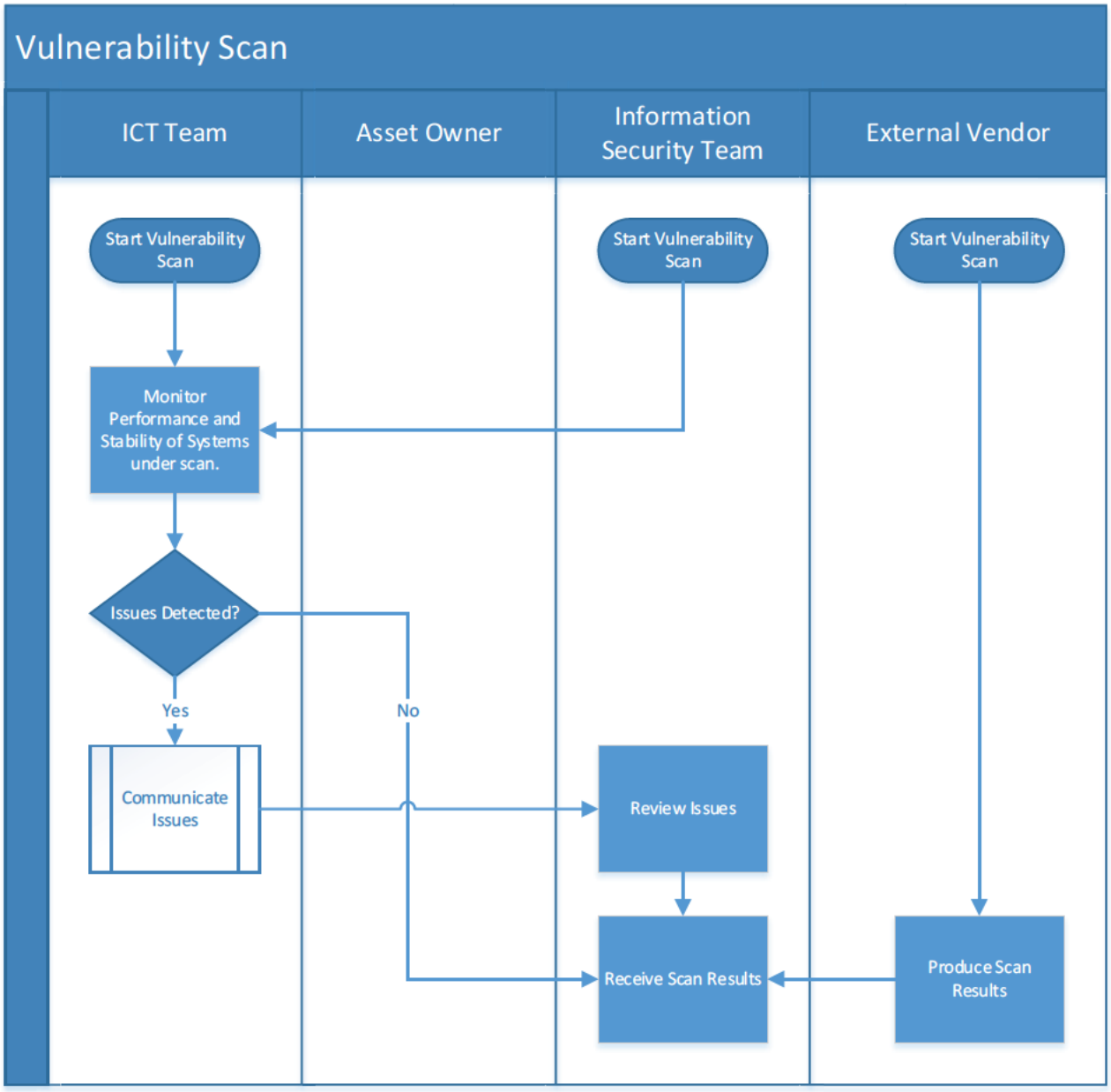
4.2.3. Vulnerability Scans

The most common path for vulnerability notifications will come through vulnerability scans. These include the initial vulnerability scan for a new deployment, scheduled internal scans (**at least weekly**), or scheduled external scans (**at least quarterly**).

A vulnerability scan may be initiated by the ICT Team, Information Security Team or an External vendor authorized to do so. Refer to *ISMS-065 Policy, Technical Compliance Review* for scanning procedures.

- During the scan, ICT will monitor network and system performance through SCOM or other monitoring systems.
    - If an issue is noted by ICT, they will escalate to the Information Security Team. They may take direct action to mitigate the incident if able.
    - If the issue can be mitigated or tolerated, the scan will be completed as normally.
- Once the scan is completed, the Information Security Team will review the Scan Results.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 581



Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 582

4.2.4. Penetration Test / Other Technical Compliance Review

Stefanini may receive notification of a vulnerability through a penetration test or other type of technical compliance review. These may require action be taken to reduce exposure or a patch may need to be applied.

Internal / External network penetration tests will be completed at least annually. Additional penetration tests will be completed as business needs require.

The Information Security Team will review the vulnerability and work with the ICT / Application teams to understand exposure. If exposure is normal, a decision will be made with the asset owner to allow the vulnerability to be corrected during a normal maintenance cycle or an acceptance of the vulnerability.

If exposure is high, a decision will be made with the asset owner on whether to perform an Emergency correction, allow it to be corrected during a normal maintenance cycle or to accept the vulnerability.

If Emergency corrective actions are authorized, an Emergency Change Order will be placed in the Stefanini Service Desk system and will follow the Change Management Process.

4.2.5. Remediation

Once the scan results are received, the Information Security Team will review the scan results. The Information Security Team is responsible for analyzing the results and making an initial determination on the associated risks.

4.2.5.1. For Initial Vulnerability Scans of New Systems

- Vulnerabilities will be evaluated per **CVSS score**.
- Any vulnerabilities listed as Critical must be remediated prior to final production deployment or external connectivity (Internet). Any vulnerabilities listed as High should be remediated prior to final production deployment.
- Scan results may be communicated through email, IM or through an Incident in Stefanini Service Desk.
- The ICT / Application Teams will work with the Asset Owner to define a Corrective Action Plan. This plan may or may not be documented.
- The Asset Owner may request that the Risk be accepted. The Information Security Team will review to ensure the exposure meets Stefanini's thresholds. The acceptance will be documented in an Incident ticket.
- Final results of corrective actions will be communicated to the Information Security Team.

4.2.5.2. For Internal Vulnerability Scans

- Vulnerabilities will be evaluated per **Tenable's VPR score**.
- Any vulnerabilities listed as Critical must be remediated or justification for a waiver must be provided. Any vulnerabilities listed as High should be remediated.

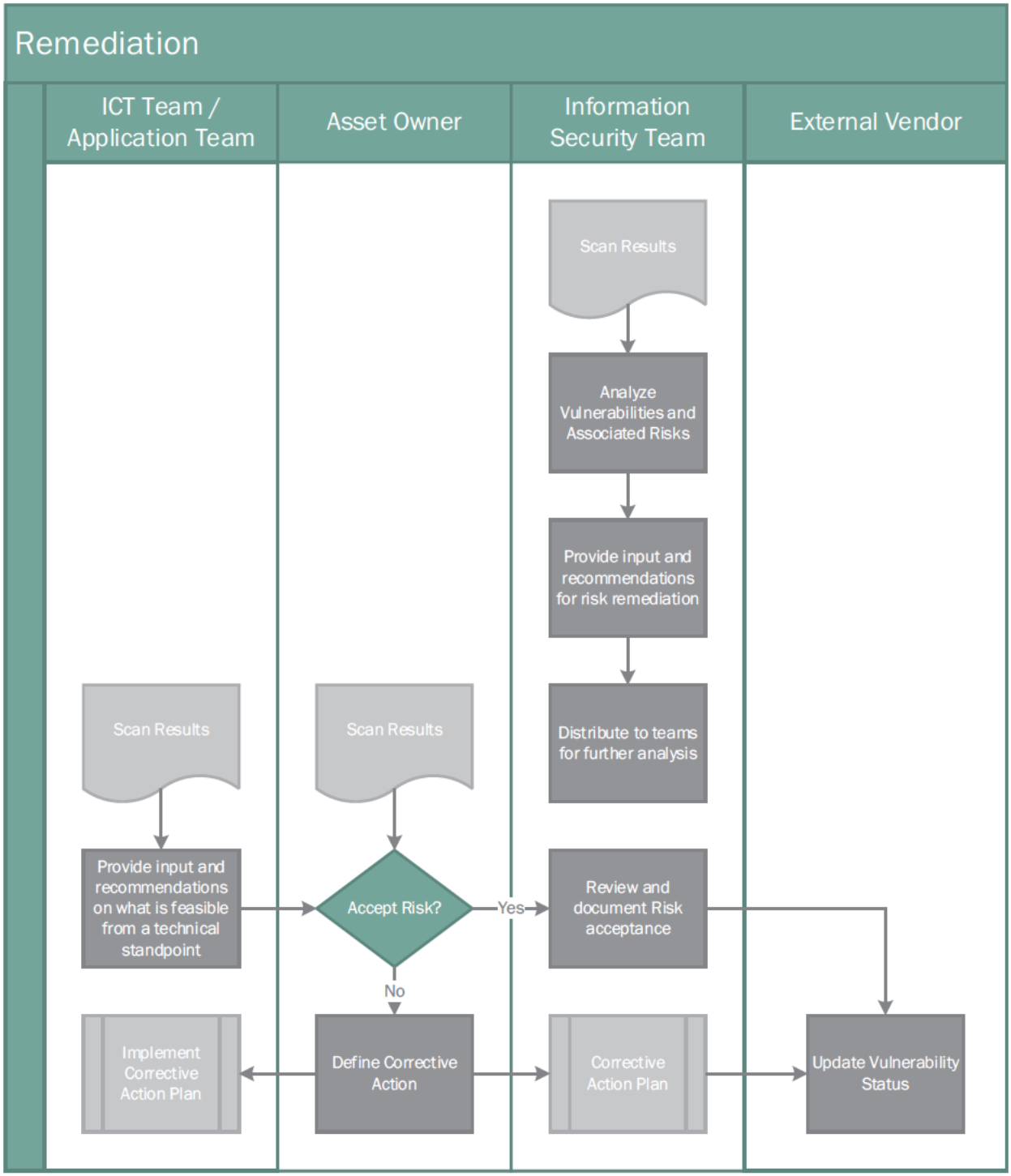
Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 583

- Scan results will be communicated through an Incident in Stefanini Service Desk.
- The ICT / Application Teams will work with the Asset Owner to define a Corrective Action Plan. This plan will be documented in the Incident. Change Orders, if required, will be created per the Change Management process.
- The Asset Owner may request that the Risk be accepted. The Information Security Team will review to ensure the exposure meets Stefanini's thresholds. The acceptance will be documented in the Incident ticket.
- Final results of corrective actions will be communicated to the Information Security Team.

4.2.5.3. For External Vulnerability Scans

- Vulnerabilities will be evaluated per **Qualys numeric score**.
- Any vulnerabilities listed as Critical must be remediated or justification for a waiver must be provided. Any vulnerabilities listed as Severe or High should be remediated.
- Scan results will be communicated through an Incident in Stefanini Service Desk.
- The ICT / Application Teams will work with the Asset Owner to define a Corrective Action Plan. This plan will be documented in the Incident. Change Orders, if required, will be created per the Change Management process.
- The Asset Owner may request that a Risk be accepted. The Information Security Team will review and update the External Vendor's vulnerability records.
- Final results of corrective actions will be communicated to the Information Security Team. The Information Security Team will review and update the External Vendor's vulnerability records.

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 584



Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 585

4.2.6. Responsibilities

Role	Responsibility
Information Security Team	The information security team is responsible for configuring the vulnerability scans and scheduling the various vulnerability scans. They are also responsible for initial evaluation and distribution of vulnerabilities.
Asset Owner	The asset owner is responsible for the ICT / Application asset that is scanned by the vulnerability management process. This role should decide whether identified vulnerabilities are mitigated or their associated risks are accepted. This role may also be responsible for final corrective action.
ICT / Application Team	The ICT and Application Teams are typically responsible for implementing remediating actions defined as a result of detected vulnerabilities. They may also provide guidance on possible corrective actions.
External Vendor	The external vendor is responsible for configuring the vulnerability scans and scheduling the various vulnerability scans as instructed.

5. Managing records kept on the basis of this document

Record name / Identification	Storage location	Responsible for Storage	Protection	Restore	Retention time	Disposal
Stefanini Service Desk Change Order	Stefanini Service Desk	Information Security Management	By AD logon	According backup policy.	3 years	Delete
Stefanini Service Desk Incident	Stefanini Service Desk	Information Security Management	By AD logon	According backup policy.	3 years	Delete
Internal Vulnerability Scan Results	Tenable Security Center	Information Security Management	By AD logon	According backup policy.	90 days	Delete
External Vulnerability Scan Results	MSSP	Information Security Management	By unique logon	According backup policy.	3 years	Delete

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 586

6. Document management

The owner of this document is the Infrastructure and Support Departments, who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria must be considered:

- Number of vulnerabilities identified
- Number of remediated vulnerabilities versus accepted risks

A current version of this document is available to all staff and under version control on the corporate document control system.

7. Appendices

- Not applicable

8. Change history

Date	Version	Created by	Description of change
22-JAN-2014	1.0	Matthew Engler	Document creation
26-AUG-2020	2.0	Matthew Engler	Added in patching process (with timing) for maintenance and patching

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 587

Agile Development Life Cycle

Document Type: Process

Applicable to: Corporate Documentation

This document is applicable to the following region(s):

- ☐ All Regions (Global)
- ☒ APAC
- ☒ EMEA
- ☒ North America



Anexo Certificação solicitada 11 (6460210) SEI 19.09.02684.0011790/2021-22 / pg. 588

stefanini
CO-CREATING SOLUTIONS FOR A BETTER FUTURE

CONFIDENTIAL INFORMATION OF STEFANINI, INC.

This document contains information that is proprietary and/or confidential to Stefanini, Inc. It is not to be disclosed, in whole or in part, without the express written authorization of Stefanini, Inc. It shall not be duplicated or used, in whole or in part, for any purpose other than the described on this document.

Copyright© Stefanini, Inc.

All Rights Reserved.

Internal Use

Doc ID	**ISMS-070NH Process, Agile Development Life Cycle**
Version	1.0 (Change history available at the end of this document
Document Owner	33004 – ICT Risk Management
Written by	Matthew Engler
Reviewed by	Elanie Pinheiro
Approved by	Washington Souza
Language version available	**English** (Mandatory and official) Additional languages available (check with Document Owner) ☐Filipino ☐Portuguese ☐Romanian ☐Spanish
Version effective from	16-Dec-2019
Next review date	03-Aug-2020
Confidentiality Level	INTERNAL USE [External access to this data is to be prevented]

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 589

Table of Contents

1 PURPOSE, SCOPE AND USERS 5

1.1 PURPOSE 5

1.2 SCOPE 5

1.3 USERS 5

2 DEFINITIONS 5

3 REFERENCES – RELATED DOCUMENTS 6

4 PROCEDURE 6

4.1 AGILE DEVELOPMENT 6

4.2 SCRUM CYCLE 6

4.2.1 Preparation 7

4.2.2 Product Backlog 7

4.2.3 Sprint Planning Meetings 8

4.2.4 Sprint Backlog 8

4.2.5 Daily Meeting 9

4.2.6 Product Increment 9

4.2.7 Definition of Done (DoD) 9

4.2.8 Sprint Review 10

4.2.9 Sprint Retrospective 10

4.3 THE SECURE SCRUM METHODOLOGY 10

4.4 ARTIFACTS 10

4.4.1 List of Impediments 11

4.4.2 Burndown 11

4.4.3 SARs Reports 11

4.5 ROLES 12

4.5.1 Scrum Master 12

4.5.2 Product Owner 12

4.5.3 Agile Team 12

4.5.4 Stakeholders 12

4.5.5 Project Manager 13

Internal Use

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 590

5 DOCUMENTED INFORMATION DETAILS 13
6 CHANGE HISTORY 14

Internal Use

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 591

1 Purpose, scope and users

1.1 Purpose

The purpose of this document is to present a system for the development of software. This system aims at structuring and standardizing the software systems development model so that the developed products are delivered with more quality, security, and reliability to Stefanini's customers.

1.2 Scope

Software development projects with new or relevant scopes developed using an Agile methodlogy.

Note: Sustaining projects, application sustaining, ongoing demands, and one-off demands do not utilize this development process despite their similarity. The method for developing these works is at the discretion of their clients.

1.3 Users

This process is applicable to Stefanini development and is intended for use by the development projects performing any of the services outlined in this document.

2 Definitions

1.1 **Intranet:** An intranet is a private network accessible only to Stefanini staff.
1.2 **"must", "shall" or "will":** Mandatory. Based on Requirement or Regulation
1.3 **"is" or "are":** Current practice at Stefanini
1.4 "may" or "can": Optional
1.5 **"should":** Best Practice

Internal Use

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 592

3 References – Related Documents

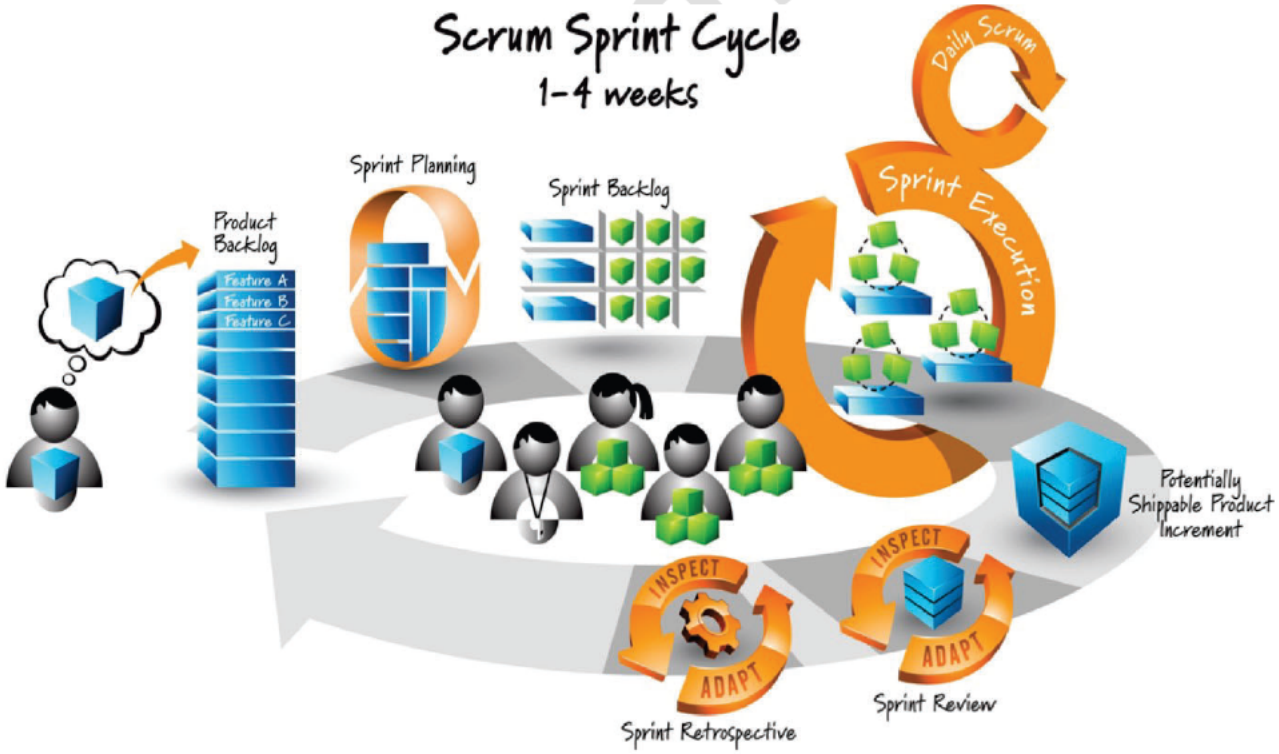
- ISO/IEC 27001 standard, A.14.1.1, A.14.2.1,
- ISMS-046 Policy, Secure Development
- ISMS-051 Policy, Server_System Security
- ISMS-066NH Security Requirements, Secure Development

4 Procedure

4.1 Agile Development

The development methodology is structured on the agile model that follows an incremental model to deliver faster customer value. There are phases, stages and activities, in which the requirements evolve throughout the project and can be changed by the end of the project (due to business needs).

4.2 Scrum Cycle



Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 593

At the beginning of the project, all known requirements are listed and stored in the Backlog, this step counts on the participation of all the necessary stakeholders so that the backlog is as faithful as possible to the company's needs. As the project progresses, new requirements can be added to the backlog and the team will find the best time for their development by evaluating the prioritization of requirements. The team estimates (time, cost and expectations) the required sprints with the agile development team. This number of Sprints is used as inputs for pricing and project duration.

Sprints are fixed periods where the agile team must deliver a set of requirements that add value to the customer's business. It is essential that every Sprint contains elements that truly deliver value to the customer and the customer must understand that value. The duration of **two weeks** is a usual suggestion.

During a Sprint, each team member has their responsibilities and updates the project kanban with their progress. Every day there is a follow-up event called the Daily Meeting whose main objective is to understand from each person what they have done, if they have encountered any obstacles and what they will do until the next meeting. Route deviations are handled at this time by the project manager or Scrum Master. At the end of a Sprint a set of features is delivered working and, generating customer value. The system is usable while not being fully finalized. This cycle repeats several times until the customer understands that the system meets their needs. In some products, this cycle may not end without continual improvement.

Typically a project contains the following tasks:

4.2.1 Preparation

This task discusses the project and awareness of the challenges of the project. The team discusses what is expected by the project and what problems and advantages are expected. In other words, how much value will the project bring to the client's business. Some inputs that can be analyzed are business case, design, initial ideas, regulatory documents and others. Based on this, the team creates or updates the backlog containing the project's functionality.

4.2.2 Product Backlog

Product Backlog is a list containing all the desired functionality for a product. The contents of this list are defined by the Product Owner. The Product Backlog does not have to be complete at the beginning of a project. You can start with all that is essential in the first phase. Over time, the Product Backlog may change as you learn more about the product and its users.

During Sprint Planning Meeting, the Product Owner prioritizes Product Backlog items and describes them to the team. The team then determines which items they will be able to complete during the upcoming Sprint. Such items are then transferred from Product Backlog to Sprint Backlog. By doing so, the team breaks each Product Backlog item into one or more Sprint

Internal Use

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 594

Backlog tasks. This helps to divide the work between team members. The Product Backlog may include technical tasks or activities directly related to the requested functionality.

4.2.3 Sprint Planning Meetings

The Sprint Planning Meeting is a meeting attended by the Product Owner, the Scrum Master, and the entire Agile Team, as well as anyone interested in representing management or the customer.

During the Sprint Planning Meeting, the Product Owner describes the highest priority features for the team. The team asks questions during the meeting so that they can break functionality into technical tasks after the meeting. These tasks will give rise to the Sprint Backlog.

The Product Owner does not need to describe all items that are in the Product Backlog. Depending on the size of the Product Backlog and the speed of the team, it may be sufficient to describe only the highest priority items, leaving the discussion of the lower priority items for the next Sprint Planning Meeting.

Collectively, the Agile Team and Product Owner set a goal for the Sprint, which is a brief description of what the Sprint will try to achieve. Sprint success will be evaluated later at the Sprint Review Meeting against the Sprint goal.

After the Sprint Planning Meeting, the Scrum team meets separately to talk about what they have heard and to decide how much they can commit to doing at the start. In some cases, there will be negotiations with the Product Owner, but it will always be the team's responsibility to determine how much they will be able to commit to doing.

4.2.4 Sprint Backlog

The Sprint Backlog is a list of tasks that the Agile Team undertakes to do in a Sprint. The Sprint Backlog items are extracted from the Product Backlog by the team based on the priorities set by the Product Owner and the team's perception of the time it will take to complete the various features.

It is up to the team to determine the amount of Product Backlog items that will be brought into the Sprint Backlog, as it will commit to implementing them.

During a Sprint, the Agile Team keeps the Sprint Backlog updated to reflect which tasks are completed and the time the team believes will be needed to complete those that are not yet done. The estimate of work that remains to be done in a Sprint is calculated daily and plotted on a chart called the Sprint Burndown Chart.

Internal Use

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 595

4.2.5 Daily Meeting

Each day of the Sprint, the team holds a meeting called the Daily Meeting. It aims to disseminate knowledge about what was done the day before, identify impediments, and prioritize the work to be done for the day ahead.

Daily Meetings are usually held at the same place at the same time of day. Ideally they are held in the morning to help set priorities for the new work day.

All team members must attend the Daily Meeting. Other people may also be present, but can only listen. This makes Daily Meetings a great way for a team to disseminate project status information.

The Daily meeting should not be used as a problem-solving meeting. Questions raised should be taken outside the meeting and usually dealt with by a smaller group of people who have a direct bearing on the problem or can contribute to solving it. During the Daily Meetiong, each team member provides answers to each of these three questions:

- What did you do yesterday?
- What are you going to do today?
- Are there any impediments to your progress?

By focusing on what each person did yesterday and what they will do today, the team gains an understanding of what work has been done and what still needs to be done. The Daily Meeting is not a status report meeting where a boss is collecting information about who is late. Instead, it is a meeting in which team members make commitments to each other.

Impediments identified in the Daily Meeting should be addressed by the Scrum Master as soon as possible.

4.2.6 Product Increment

The increment is the sum of all completed Product Backlog items. At the end of a Sprint, the new increment must be "ready", meaning that it is in a usable condition and meets the definition given by the Definition of Done (DoD) team.

4.2.7 Definition of Done (DoD)

The result of a Sprint is the completed product or functionality.

To know when, and how, a part of the product or functionality should be considered complete is a document called Definition of Done.

Although this varies significantly from end to end for each agile team, team members must have a shared understanding of what it means to be complete, ensuring transparency. This is the "Ready Setting" for the Agile Team and is used to ensure when work is completed on the product increment.

Internal Use

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 596

4.2.8 Sprint Review

At the end of each Sprint, a Sprint Review Meeting is held. During this meeting, the Agile Team shows what was achieved during the sprint. Typically this has the format of a demo of the new features.

Sprint Review participants typically include Product Owner, Agile Team, Scrum Master, management, customers, and engineers from other projects.

During the Sprint Review, the project is evaluated against the Sprint objectives determined during the Sprint Planning Meeting. Ideally, the team completed each of the Product Backlog items brought in as part of Sprint, but the important thing is that the team achieves the Sprint's overall goal.

4.2.9 Sprint Retrospective

Sprint Retrospective occurs at the end of a Sprint and serves to identify what worked well, what can be improved, and what actions will be taken to improve it.

4.3 The Secure Scrum Methodology

Successfully implementing strong application security is one of the most challenging non-functional tasks Scrum teams face. It is important to define and link security risks to user stories in the Product Backlog.

The following adaptions to the Agile methodology must be considered:

- **Identification** is the process which diagnoses potential security concerns throughout the application development process. Practically, this is accomplished by marking items in the Product Backlog when security concerns are discovered. The identification process occurs during Product Backlog creation, Product Backlog Refinement, Sprint Planning, and Sprint Reviews.
- **Implementation** is the process which ensures security concerns are properly understood by the development team and is carried out during Sprint Planning and Daily Scrum meetings.
- **Verification** evaluates an application's security is run during Daily Scrums.
- **Definition of Done** represents a criteria which establishes the threshold for completion with regards to resolving an application security concern.

4.4 Artifacts

One of the hallmarks of agile designs is the generation of value-adding artifacts only. Teams follow the agile manifesto that says, "Running software more than comprehensive

Internal Use

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 597

documentation," and investing more time in producing code that delivers customer value than documents that may not generate immediate business benefit.

4.4.1 List of Impediments

An impediment is anything that might hinder the Scrum team's performance in achieving its expected goals. This is usually an atypical situation that is beyond the control of the team and needs further investigation or work to resolve it. Some impediments can even paralyze parts of projects. The list of impediments is a document available to everyone, so that the team can help themselves to resolve the impediments. It must be clear and objective, and contain all impediments encountered.

Common examples of impediments:

- Ad-hoc meetings
- Team member illness
- Failure to fulfill commitments by third parties or partners
- Lack of equipment like computer and others
- Low Product Owner Dedication
- Lack of management support (management may not trust team)
- Technical question
- Team Member Conflicts
- Above-normal bureaucracy

4.4.2 Burndown

In an Agile project, the team monitors its progress against a plan by updating a Release Burndown Chart at the end of each Sprint (iteration). The horizontal axis of a Release Burndown Chart shows Sprints; The vertical axis shows how much work still needs to be done at the beginning of each Sprint. The remaining work can be shown in the team's preferred unit: story points, ideal days, team days, and so on.

During a Sprint, the agile team keeps the Sprint Backlog up to date to reflect what tasks are completed and how long they believe it will take to complete those that are not yet done. The estimate of work that remains to be done on the Sprint is calculated daily and plotted, resulting in a Sprint Burndown Chart.

4.4.3 SARs Reports

Throughout the project, managers can track various aspects of performance through SARs (Stefanini Agile Reports). This tool provides support to bring more dynamic and objective information to project managers and team members. From the available resources you can view team performance, velocity, lead time, and status of each Sprint.

Internal Use

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 598

4.5 Roles

4.5.1 Scrum Master

The Scrum Master seeks to ensure that the team respects and follows the agile values and practices adopted for the project. It also protects the team by ensuring that it does not overly commit to what it can accomplish during a sprint.

The Scrum Master acts as a facilitator of the impediments raised at the Daily Meeting and becomes responsible for removing any obstacles that are raised by the staff during these meetings.

The role of Scrum Master is typically performed by a project manager or a technical leader, but in principle can be anyone on the team.

4.5.2 Product Owner

The Product Owner is the person who defines the items that make up the Product Backlog and prioritizes them in Sprint Planning Meetings.

The team commits to performing a set of activities in each Sprint and the Product Owner commits not to bring new requirements to the team during the Sprint. Requirements may change (and changes are encouraged), but only outside of a Sprint. Once the team starts working on a Sprint, it remains focused on the Sprint goal and new requirements are not accepted.

4.5.3 Agile Team

Agile Team is the development team. In it, there is not necessarily a functional division across traditional roles, such as programmer, designer, test analyst, or architect. Everyone in the project works together to complete the working set they have jointly committed to for a Sprint.

A typical Agile Team has between 6 and 10 people, although there are reports of Scrum projects with larger teams.

4.5.4 Stakeholders

Stakeholders can generally be consulted to check the project vision and even validate its alignment as it is worth remembering that Stakeholders are the main stakeholders in the project.

Typically stakeholders are people in positions such as the company's board of directors, senior managers, customers and users. The team is also a stakeholder, but their commitment is often less business and more technical.

Internal Use

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 599

4.5.5 Project Manager

The Project Manager in Agile Environments is the professional responsible for end-to-end project costs and monitoring, being on the agile team for one or more projects. They must be multidisciplinary and have some skills such as: negotiation techniques, commitment, organization, leadership, communication, problem solving and decision making. One of the project manager's main activities in this environment is as a negotiator and moderator of potential conflicts.

5 Documented Information Details

Record name / Identification	Storage location	Responsible for Storage	Protection	Restore	Retention time	Disposal
Project	SharePoint	Project Manager	By AD Login	According to backup policy	6 months following project completion	Delete
List of Impediments	SharePoint	Project Manager	By AD Login	According to backup policy	Duration of Project	Delete
Product Backlog	Jira	Project Manager	By Jira Login	According to backup policy	Duration of Project	Delete
Sprint Backlog	Jira	Project Manager	By Jira Login	According to backup policy	Duration of Project	Delete
Burndown	Jira	Project Manager	By Jira Login	According to backup policy	Duration of Project	Delete
Specifications	SharePoint	Project Manager	By AD Login	According to backup policy	Duration of Project	Delete
Architecture	SharePoint	Project Manager	By AD Login	According to backup policy	6 months following project completion	Delete
Source Code	Git	Project Manager	By Git Login	According to backup policy	6 months following project completion	Delete

Internal Use

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 600

Test Evidence	SharePoint	Project Manager	By AD Login	According to backup policy	6 months following project completion	Delete
Acceptance	SharePoint	Project Manager	By AD Login	According to backup policy	6 months following project completion	Delete

6 Change history

Date	Version	Written by / Reviewed by	Notes	Approved by
2-Dec-2019	1.0	Matthew Engler	Initial creation.	Full Name
Click or tap to enter a date.				
Click or tap to enter a date.				
Click or tap to enter a date.				
Click or tap to enter a date.				

Internal Use

Anexo Certificação solicitada 11 (0180210) SEI 19.09.02684.0011790/2021-22 / pg. 601

ENC: Questionamento da área de Contratos do MPBA

Patricia Goncalves Maia Dantas <pmdantas@stefanini.com>

Sex, 13/08/2021 09:54

Para: Iaçanã Lima de Jesus Carneiro <iassa@mpba.mp.br>

Iaçanã,

Para otimizar a procuração, Marco e Graça fizeram uma procuração contendo várias empresas do grupo da qual eles são sócios e deram poderes para assinar para a Magali. A Stefanini Rafael é o item 3 da procuração.

PROCURAÇÃO BASTANTE QUE FAZ: ORBITALLSERVIÇOS E PROCESSAMENTO DE MEIOS DEPAGAMENTO LTDA e outros

SAIBAM quantos este público instrumento de procuração bastante virem que, aos trinta e um (31) dias do mês de maio do ano de dois mil e vinte e um (2021), neste Oficial do Registro Civil das Pessoas Naturais do 39º Subdistrito Vila
Madalena, por vídeo conferência nos termos do Provimento 100 do CNJ, perante mim, SUBSTITUTA, compareceram como outorgantes:

[...]

3) STEFANINI RAFAEL SEGURANÇA E DEFESA S.A., sociedade anônima,
inscrita no CNPJ/MF de nº 24.691.488/0001-09, com sede na Avenida Eusébio Matoso, 1375, 8º andar, salas 801 e 802, Butantã, CEP 05423-905, São Paulo, SP, com seu Estatuto Social Consolidado, anexo a Ata da Assembleia Geral Extraordinária, realizada aos 09/01/2017, devidamente registrada na Junta Comercial do Estado de São Paulo (JUCESP) aos 24/02/2017, sob nº 106.436/17-0 e Certidão Simplificada Eletrônica, emitida pela Junta
supramencionada, aos 16/04/2021, autenticidade nº 150428367, neste ato representada nos termos dos ARTIGOS 13, 18 - Parágrafo 1º, 19 - Parágrafo 1º, do documento supracitado, cuja cópia fica arquivada nesta Serventia em Pasta Própria (CS 70, fls. 58), pelos Diretores eleitos conforme Instrumento Particular de 1ª Alteração ao Contrato Social e Assembleia Geral de Transformação, datado de 10/05/2016, devidamente registrado na Junta Comercial do Estado de São Paulo (JUCESP), aos 24/06/2016, sob nº 3530049265-0: MARCO ANTONIO SILVA STEFANINI, brasileiro, casado, empresário, portador da cédula de identidade RG nº 10.153.181-3 SSP/SP, inscrito no CPF/MF sob nº 042.501.968-36, residente e domiciliado na Rua Marcos Melega, 150 - 3H, Edifício Casuarina - Alto de Pinheiros, São Paulo – SP, CEP 05466-010, MARIA DAS GRAÇAS VUOLO SAJOVIC STEFANINI, brasileira, casada, empresária, portadora da cédula de identidade RG nº 8.546.223-8 SSP/SP, inscrita no CPF/MF sob nº 15.819.138-26, residente e domiciliada na Rua Marcos Melega, 150 - 3H, Edifício Casuarina, Alto de Pinheiros, São Paulo – SP, CEP 05466-010;

Se precisarem de qualquer complemento de informação favor entrar em contato.

Anexo E-mail Stefanini (0180214) SEI 19.09.02684.0011790/2021-22 / pg. 602

PATRÍCIA MAIA DANTAS
Diretora Negócios - Governo

-
+ 55 71 99624-7432

www.stefanini.com

De: Iaçanã Lima de Jesus Carneiro <iassa@mpba.mp.br>
Enviada em: quinta-feira, 12 de agosto de 2021 16:45
Para: Patricia Goncalves Maia Dantas <pmdantas@stefanini.com>
Assunto: Questionamento da área de Contratos do MPBA

[EXTERNAL EMAIL]

Patricia, boa tarde!

Segue para conhecimento e providencias do quanto exposto abaixo pela área de contratos:

"*... Verificamos que na Procuração constante no procedimento (0169642) Maria Magali Bredariol, cujo documento de identidade se encontra no expediente (0165289), tem poderes outrogados apenas pela empresa ORBITALL ATENDIMENTO LTDA. Além da referida outrorgante não ser a empresa indicada como contratada, a supracitada Procuradora somente poderia agir em conjunto com um Diretor ou com outro Procurador devidamente constituído no que diz respeito à representação da empresa em contratações com pessoas físicas ou jurídicas.*"

Ficamos no aguardo, grato pela atenção.

Cordialmente

Iaçanã L. J. Carneiro | Tel. (71) 3103-0212 / 0214

CASI - Coordenação de Assessoramento em Segurança da informação

Anexo E-mail Stefanini (0180214) SEI 19.09.02684.0011790/2021-22 / pg. 603

http://www.mpba.mp.br

Importante: As informações deste e-mail são confidenciais. O uso não autorizado é proibido por lei. Por favor, considere o ambiente antes de imprimir.

Important: The information on this e-mail is confidential. Non-authorized use is prohibited by law. Please Consider the Environment Before Printing.

Anexo E-mail Stefanini (0180214) SEI 19.09.02684.0011790/2021-22 / pg. 604

1. OBJETO		
1.1 DEFINIÇÃO DO OBJETO	**Especificação do Objeto** Contratação de serviços realização de PENTEST (teste de invasão) na abordagem Blackbox na aplicação Voto Eletrônico. **Observação**: Detalhamento dos itens que compõem o objeto constam na tabela 1 do ANEXO I (indicado ao final do documento).	
1.2 FORMA DE CONTRATAÇÃO ESCOLHER UMA DAS TRÊS OPÇÕES ***(Marcar com X)***:	**(x)**	**A) PRESTAÇÃO DE SERVIÇOS IMEDIATA (PONTUAL/POR ESCOPO)**
	( )	**B) PRESTAÇÃO DE SERVIÇOS PARCELADA**
	( )	**C) PRESTAÇÃO DE SERVIÇOS SOB DEMANDA**
	( )	**D) OUTROS:**
1.3 JUSTIFICATIVA: **NECESSIDADE DA CONTRATAÇÃO**	O Ministério Público do Estado da Bahia (MPBA) encontra-se em plena transformação digital, passando por mudança de cultura e adoção de novos procedimentos que estão sendo alicerçados pela tecnologia da informação. Neste contexto, a Alta Administração da instituição decidiu pela realização das eleições internas através de sistema informatizado de votação denominado VOTO DIGITAL. Originalmente cedido pelo Ministério Público do Estado de São Paulo com o nome VOTO ELETRÔNICO, o sistema foi instalado e configurado no ambiente tecnológico do MPBA e posteriormente adaptado para funcionar de acordo com as regras estabelecidas pelos seus gestores, passando a ser chamado de VOTO DIGITAL. De forma inovadora, será possibilitado que os membros do MPBA possam votar a partir de computadores ou dispositivos móveis conectados à *internet*, mediante dupla autenticação e outros requisitos de segurança. É sabido que os processos eleitorais são sujeitos a críticas ainda mais quando envolvem tecnologia da informação e comunicação. Objetivando garantir a máxima segurança da informação possível no sistema VOTO DIGITAL, o MPBA vem realizando ações tecnológicas e procedimentais visando garantir a lisura e transparência de todo o processo eleitoral assim como das ferramentas tecnológicas envolvidas.	

	O MPBA entende que a realização de um Teste de Intrusão - PENTEST -, conjunto de testes visando detectar falhas e/ou vulnerabilidades da referida aplicação e na infraestrutura que a suporta, utilizando técnicas dos Hackers éticos - especialistas em segurança da informação, irá possibilitar o conhecimento maior sobre a aplicação e sua infra com o intuito de ter um ambiente o mais seguro possível, atendendo aos princípios basilares da segurança da informação - Integridade, Confiabilidade e Disponibilidade. A presente contratação visa a realização de uma análise independente e externa a área de TI do MPBA com o objetivo de eliminar eventuais vulnerabilidades do sistema VOTO DIGITAL contribuindo para que o mesmo seja executado de maneira segura.
1.4 JUSTIFICATIVA: **QUANTITATIVO(S) DEFINIDO(S)**	Será realizado um Pentest completo – testes, mitigações de possíveis vulnerabilidades encontrada, reteste para assegurar que as vulnerabilidades foram devidamente mitigadas, durante o prazo da contratação para a aplicação Voto Eletrônico. Assim se tem de forma inequívoca que os requisitos de proteção a aplicação, na esfera dos testes de intrusão, foram atendidos.

1.5 INDICAÇÃO DE MODELO E/OU MARCA OBRIGATÓRIOS ESCOLHER UMA OPÇÃO* ***(Marcar com X)***:	**( )** SIM	**(x)** NÃO
	1.5.1 INDICAÇÃO DO(S) ITEM(NS) E DO MODELO/MARCA - Em caso positivo:	
	1.5.2 JUSTIFICATIVA PARA CADA ITEM - Em caso positivo:	

2. FUNDAMENTO LEGAL

2.1 INDICAÇÃO DO DISPOSITIVO LEGAL EM QUE SE ENQUADRA A HIPÓTESE DE CONTRATAÇÃO ESCOLHER UMA OPÇÃO* ***(Marcar com X)***:	**( )**	**A) Artigo 59, I da Lei Estadual/BA nº 9.433/2005** - para obras e serviços de engenharia de valor não excedente a 10% (dez por cento) do limite previsto para modalidade de convite, desde que não se refiram a parcelas de uma mesma obra ou serviço, ou ainda para obras e serviços da mesma natureza e no mesmo local que possam ser realizadas conjunta e concomitantemente;
	(x)	**B) Artigo 59, II da Lei Estadual/BA nº 9.433/2005** - para serviços e compras de valor até 10% (dez por cento) do limite previsto para compras e serviços que não sejam de engenharia, na modalidade de convite, e para alienações, nos casos previstos nesta Lei, desde que não se refiram a parcelas de um mesmo serviço, compra ou alienação de maior vulto que possa ser realizada de uma só vez;

	( )	C) **OUTROS**

3. REGRAS DE CONTRATAÇÃO

3.1 REGRAS DE FORMALIZAÇÃO CONTRATUAL	**3.1.1 HAVERÁ CELEBRAÇÃO DE CONTRATO** **(x) A SIM** **( ) B NÃO (FORMALIZAÇÃO SE DARÁ APENAS COM A EMISSÃO DE EMPENHO)**
3.2 REGRAS DE EXECUÇÃO CONTRATUAL	**3.2.1 REGIME DE EXECUÇÃO:** **( ) Empreitada por preço** **(x) Empreitada por preço global** **( ) Outro:** **3.2.2 PRAZO PARA RETIRADA DA NOTA DE EMPENHO:** ➢ 5 dias **( )** Úteis **(x)** Corridos. ➢ Contados da convocação pelo Ministério Público, a ser formalizada preferencialmente por e-mail. **3.2.3 PRAZOS DE EXECUÇÃO** ➢ 30 dias **( )** Úteis **(x)** Corridos ➢ O prazo será contado da data do recebimento, pelo Fornecedor, da Nota de Empenho, acompanhada da autorização de fornecimento e, se for o caso, do instrumento contratual.

3.2.4 ADMISSIBILIDADE DE PRORROGAÇÃO DO PRAZO DE EXECUÇÃO

( )	**A) NÃO**
(x)	**B) SIM.** Neste caso, somente será admissível o pedido formalizado pelo fornecedor antes do termo final do prazo de entrega consignado, mediante justificativa - e respectiva comprovação - de fato superveniente, aceito pela Instituição. ➢ Por até 30 dias **(x)** Úteis **( )** Corridos

3.2.5 LOCAL DE EXECUÇÃO DOS SERVIÇOS: Os serviços contratados deverão ser obrigatoriamente executados de fora das dependências da CONTRATANTE, simulando o quanto

3.2 REGRAS DE EXECUÇÃO CONTRATUAL	possível um ataque real, conforme modelo Blackbox do pentest solicitado. A entrega do produto final, o relatório das vulnerabilidades encontradas e mitigadas, será apresentado em reunião por vídeo conferência e enviado por e-mail para casi@mpba.mp.br. **3.2.6 REGRAS ESPECIAIS PARA EXECUÇÃO:** ➢ Execução deve ser agendada - ESCOLHER UMA OPÇÃO ***(Marcar com X)***: **( )** A) NÃO **(x)** B) SIM ➢ Unidade responsável: Diretoria de Tecnologia da Informação ➢ Telefone e e-mail para contato e/ou agendamento: (71) 3103-0214 e casi@mpba.mp.br ➢ Dias para realização da entrega dos serviços: Durante o mês de outubro de 2021 ➢ Horários para execução: Pela natureza do serviço serão acertados a posteriori quando da execução. ➢ Condições especiais adicionais: Não há

3.3 GARANTIA DO OBJETO ESCOLHER UMA OPÇÃO * ***(Marcar com X)***:	**(x)**	**A) SEM EXIGÊNCIA DE GARANTIA**
	( )	**B) COM EXIGÊNCIA DE GARANTIA** - Regras: ➢ **EXECUTOR DA GARANTIA** - ESCOLHER UMA OPÇÃO ***(Marcar com X)***: **( )** A) CONTRATADA (Regra geral) **( )** B) FABRICANTE (Exceção) ➢ Justificar a exigência de garantia do fabricante (Em caso positivo): ➢ **DURAÇÃO** - ESCOLHER UMA OPÇÃO ***(Marcar com X)***: **( )** A) 01 ANO **( )** B) 90 DIAS (GARANTIA LEGAL) **( )** C) OUTRO. Especificar:

		➢ **PRAZO MÁXIMO PARA RESOLUÇÃO DO CHAMADO, contado a partir da abertura pelo MPBA** - ESCOLHER UMA OPÇÃO ***(Marcar com X)***: **( )** A) _____ HORAS **( )** Úteis **( )** Corridas **( )** B) _____ DIAS **( )** Úteis **( )** Corridos ➢ **NECESSIDADE DE ASSISTÊNCIA TÉCNICA** - ESCOLHER UMA OPÇÃO ***(Marcar com X)***: **( )** A) SIM **(x)** B) NÃO ➢ **FORMA DE EXECUÇÃO DA ASSISTÊNCIA TÉCNICA** (Se resposta positiva acima) - ESCOLHER UMA OPÇÃO ***(Marcar com X)***: **( )** A) Assistência sediada na zona urbana ou metropolitana de Salvador **( )** B) Assistência sediada em local a critério do fornecedor (regra geral) **( )** C) *On site*, isto é assistência prestada diretamente na sede do MPBA (exceção). Regras: ○ Os chamados para Assistência Técnica deverão ser atendidos no prazo máximo de _____ (_____) horas, contadas da notificação pelo MPBA; ○ O Fornecedor ou Fabricante (conforme regra de "Executor" acima indicada) arcará com todas as despesas decorrentes da reparação e/ou substituição de bens, a incluir o deslocamento de seus técnicos aos locais em que aqueles estiverem, bem como pelo transporte para sua oficina, se necessário; **( )** D) Outra. Especificar: ➢ **DEMAIS REGRAMENTOS**:
3.4 CONDIÇÕES E RESPONSÁVEIS PELO RECEBIMENTO *	**3.4.1 PRAZO PARA RECEBIMENTO PROVISÓRIO:** 5 dias **( )** Úteis **(X)** Corridos	
	3.4.2 PRAZO PARA RECEBIMENTO DEFINITIVO: 10 dias **( )** Úteis **(X)** Corridos	
	3.4.3 UNIDADE RESPONSÁVEL PELO RECEBIMENTO: Diretoria de Tecnologia da Informação	
	3.4.4 PRAZO PARA ADEQUAÇÃO OU REFAZIMENTO DE SERVIÇO(S) REJEITADO(S) - ESCOLHER UMA OPÇÃO ***(Marcar com X)***: **(X)** A) NÃO SE APLICA	

	( ) B) PRAZO: ( ) _____ HORAS ( ) Úteis ( ) Corridas ( ) _____ DIAS ( ) Úteis ( ) Corridos	
	DEMAIS REGRAMENTOS: 3.4.5 O recebimento dos serviços ocorrerá mediante conferência destes, confrontando com as especificações contidas no Termo de Referência e Contrato (inclusive anexos) e na proposta de preços, bem com as quantidades determinadas na Ordem de serviços/Nota de Empenho. 3.4.6 O recebimento dado pelo Ministério Público do Estado da Bahia em fatura (ou documento afim) apresentada por transportadora a serviço do fornecedor não será considerado para fins de recebimento provisório/definitivo; 3.4.7 O recebimento definitivo do objeto deste contrato só será concretizado depois de adotados, pelo Ministério Público do Estado da Bahia, todos os procedimentos contidos nos Ato Normativos internos relativos ao tema, respeitadas as exigências contidas do art. 161 da Lei Estadual- BA nº 9.433/2005; 3.4.8 O aceite ou aprovação do objeto pelo Ministério Público do Estado da Bahia não exclui a responsabilidade do fornecedor por vícios, defeitos ou disparidades com as especificações estabelecidas neste Contrato e no processo de Dispensa Licitação que o originou, verificadas posteriormente, garantindo-se ao Ministério Público do Estado da Bahia, inclusive, as faculdades previstas na Lei Federal n.º 8.078/90 – Código de Defesa do Consumidor.	
3.5 POSSIBILIDADE OU NÃO DE SUBCONTRATAÇÃO ESCOLHER UMA OPÇÃO *(Marcar com X)*:	**(X)**	**A) VEDADA A SUBCONTRATAÇÃO**
	( )	**B) ADMITIDA A SUBCONTRATAÇÃO DE SERVIÇOS ACESSÓRIOS.** ➢ Indicar parcela(s) subcontratável(eis): ➢ Indicar regras/condições para subcontratação:
3.6 CONDIÇÕES DE PAGAMENTO	**3.6.1 PERIODICIDADE DE PAGAMENTO** - ESCOLHER UMA OPÇÃO *(Marcar com X)*:	
	(X)	**A) PAGAMENTO INTEGRAL, AO FINAL DA EXCUÇÃO E RECEBIMENTO DOS SERVIÇOS**
	( )	**B) CADA PEDIDO (E CONSEQUENTE EMPENHO EMITIDO) SERÁ PAGO INTEGRALMENTE, EM PARCELA ÚNICA**

( )	**C) PAGAMENTO PARCELADO:** ➢ Quantidade de parcelas: ➢ Definição dos montantes das parcelas (Por quantidades ou percentuais, conforme regime de execução e regramentos eventualmente definidos no anexo mencionado no item 1.2.):
( )	**C) PAGAMENTO MENSAL**
( )	**D) OUTRA:**

3.6.2 CONDIÇÕES ESPECIAIS PARA EFETIVAÇÃO DO PAGAMENTO - ESCOLHER UMA OPÇÃO ***(Marcar com X)***:

(X)	**A) NÃO SE APLICA**
( )	**B) CONDIÇÕES ESPECIAIS. Especificar:**

3.6.3 DEMAIS REGRAS:

3.6.3.1 O pagamento será processado mediante apresentação, pela contratada, de nota fiscal e certidões cabíveis - documentação esta que deverá estar devidamente acompanhada do ACEITE pelo Ministério Público do Estado da Bahia, e se concluirá no prazo de 08 (oito) dias úteis a contar da data de apresentação da documentação, desde que não haja pendência a ser regularizada;

3.6.3.2 Verificando-se qualquer pendência impeditiva do pagamento, será considerada como data de apresentação da documentação aquela na qual foi realizada a respectiva regularização;

3.6.3.3 As notas fiscais deverão discriminar os tributos, com respectivos valores, alíquotas e bases de cálculo, que tenham como fato gerador o objeto contratado;

3.6.3.4 O Ministério Público do Estado da Bahia realizará a retenção de impostos ou outras obrigações de natureza tributária, na hipótese de figurar como substituto tributário, de acordo com a legislação vigente;

3.6.3.5 Os pagamentos serão efetuados através de ordem bancária, para crédito em conta corrente e agência indicadas pela empresa contratada, preferencialmente em banco de movimentação oficial de recursos do Estado da Bahia;

3.6.3.6 A atualização monetária dos pagamentos devidos pelo Ministério Público do Estado da Bahia, em caso de mora, será calculada considerando a data do vencimento da obrigação e do seu efetivo pagamento, de acordo com a variação do INPC do IBGE pro rata tempore, observado, sempre, o disposto no item 3.6.3.2.

	3.6.3.7 A entrega do Relatório de testes é indispensável ao recebimento do objeto deste instrumento, nos termos definidos neste instrumento	
3.7 POSSIBILIDADE OU NÃO DE REAJUSTAMENTO, COM INDICAÇÃO DE ÍNDICE OFICIAL ESCOLHER UMA OPÇÃO * ***(Marcar com X):***	**(X)**	**A) PREÇOS IRREAJUSTÁVEIS**
	( )	**B) PREÇOS PASSÍVEIS DE REAJUSTAMENTO.** Regras: ➢ Índice oficial para o cálculo da variação de preços - ESCOLHER UMA OPÇÃO ***(Marcar com X)***: **( )** A) INPC/IBGE **( )** B) OUTRO. Indicar: ➢ A eventual concessão de reajustamento fica condicionada à apresentação de requerimento formal pelo Fornecedor, após o transcurso do prazo de 12 (doze) meses, contados da data da apresentação da proposta; ➢ Na hipótese de reajustamento, adotar-se-á como referencial o acumulado de 12 (doze) meses, sendo o termo inicial o mês de apresentação da proposta e termo final o mês que antecede a data de aniversário. ➢ Serão objeto de reajuste apenas os valores relativos a pedidos de serviços formalizados após o decurso do prazo de 12 (doze) meses, contados da apresentação da proposta;
3.8 DEFINIÇÃO DE VIGÊNCIAS *	**3.8.1 DEFINIÇÃO DE VIGÊNCIA DA CONTRATAÇÃO** - ESCOLHER UMA OPÇÃO ***(Marcar com X):***	
	( )	**A) CONTRATAÇÕES SEM INSTRUMENTO FORMAL DE CONTRATO** ➢ ESCOLHER UMA OPÇÃO ***(Marcar com X):*** **( ) Opção 1:** _____ meses , contados do recebimento do empenho pelo fornecedor **( ) Opção 2:** _____ dias, contados do recebimento do empenho pelo fornecedor
	(X)	**B) CONTRATAÇÕES COM INSTRUMENTO FORMAL DE CONTRATO** ➢ ESCOLHER UMA OPÇÃO ***(Marcar com X):*** **( ) Opção 1:** _____ meses, contados a partir de(a) - ESCOLHER UMA OPÇÃO ***(Marcar com X):*** **( )** A) Data certa: ____ de _____ de _____

		( ) B) Da data da publicação do resumo do contrato no Diário da Justiça Eletrônico **(x) Opção 2**: 90 dias, contados a partir de(a) - ESCOLHER UMA OPÇÃO *(Marcar com X):* ( ) A) Data certa: ____ de _____ de _____ (x) B) Da data da publicação do resumo do contrato no Diário da Justiça Eletrônico ➢ Justificar vigência superior a 12 (doze) meses (se for o caso):
	3.8.2 POSSIBILIDADE DE PRORROGAÇÃO DE PRAZO DE VIGÊNCIA - ESCOLHER UMA OPÇÃO *(Marcar com X):*	
	( )	**A) NÃO**
	(x)	**B) SIM.** Justificativa: Diante da eventual necessidade de dilação da execução contratual faz-se necessário prever a possibilidade de prorrogação do prazo de vigência.
3.9 OBRIGAÇÕES DA CONTRATADA*	**OBRIGAÇÕES GERAIS** 3.9.1 Executar o objeto contratual de acordo com os prazos e as especificações técnicas constantes no instrumento convocatório e seus anexos, no local determinado, nos dias e nos turnos e horários de expediente do MPBA, não podendo eximir-se da obrigação, ainda que parcialmente, sob a alegação de falhas, defeitos ou falta de pessoal, materiais e/ou peças; 3.9.2 Adotar as providências legais e/ou contratuais cabíveis, nas ocorrências de danos no decurso do uso normal do produto durante o prazo de garantia e por defeitos de fabricação; 3.9.3 Promover, às suas expensas e sob sua responsabilidade, a adequada embalagem, transporte e entrega do(s) bem(ns); 3.9.4 Prestar diretamente o objeto contratado, não o transferindo a outrem, no todo ou em parte, ressalvando-se apenas os casos de cisão, fusão ou incorporação da empresa contratada, desde que não impeçam os compromissos assumidos para com o **MPBA**, observando-se, ainda, eventuais restrições à subcontratação definidas neste instrumento; 3.9.5 Manter durante toda a execução da contratação, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas no procedimento de contra; 3.9.6 Providenciar e manter atualizadas todas as licenças e alvarás junto às repartições competentes que, porventura, sejam necessários à execução da contratação;	

3.9.7 Responsabilizar-se pelo cumprimento das exigências previstas na legislação profissional específica e pelos encargos fiscais e comerciais resultantes da execução da contratação;

3.9.7.1 A eventual retenção de tributos pelo **MPBA** não implicará na responsabilização deste, em hipótese alguma, por quaisquer penalidades ou gravames futuros, decorrentes de inadimplemento(s) de tributos pela empresa contratada;

3.9.8 Emitir notas fiscais/faturas de acordo com a legislação e com este documento, contendo descrição dos serviços, indicação de quantidades, preços unitários e valor total;

3.9.9 Arcar, quando da execução do objeto contratado, com todo e qualquer dano ou prejuízo, independentemente da natureza, causado ao **MPBA** e/ou a terceiros, ainda que por sua culpa, em consequência de erros, imperícia própria ou de auxiliares que estejam sob sua responsabilidade, bem como ressarcir ao **MPBA** todos os custos decorrentes de indevida paralisação ou interrupção dos serviços contratados;

3.9.10 Não introduzir, seja a que título for, nenhuma modificação na especificação do objeto contratado ou das eventuais normas técnicas a serem seguidas, sem o consentimento prévio, e por escrito, do **MPBA**;

3.9.11 Atender, nos prazos consignados neste instrumento e/ou pelo **MPBA**, às recusas ou determinações de desfazimento/refazimento fornecimentos e/ou serviços acessórios que não estejam sendo ou não tenham sido executados de acordo com as Normas Técnicas e/ou em conformidade com as condições do Edital (e anexos) constante no processo que o originou, providenciando sua imediata correção ou realização, sem ônus para o **MPBA**;

3.9.12 Permitir e oferecer condições para a mais ampla e completa fiscalização durante a vigência da contratação, fornecendo informações, propiciando o acesso à documentação pertinente e à execução contratual, e atendendo às observações e exigências apresentadas pela fiscalização;

3.9.13 Comunicar formalmente ao **MPBA** qualquer anormalidade que interfira no bom andamento da execução da contratação;

3.9.14 Manter sob sua exclusiva responsabilidade toda a supervisão e direção da eventual mão de obra necessária à execução completa e eficiente da contratação;

3.9.15 Prestar todos os esclarecimentos que forem solicitados pelo **MPBA**.

3.9.16 Acompanhar e informar sobre as atualizações tecnológicas necessárias para executar os serviços adquiridos, realizando as ações necessárias para a implantação dessas atualizações em comum acordo com o CONTRATANTE, até o final do contrato, sem ônus para o CONTRATANTE".

OBRIGAÇÕES ESPECÍFICAS (DEFINIDAS EM RAZÃO DO OBJETO CONTRATADO):

	( )	**A) NÃO EXISTEM OBRIGAÇÕES ESPECÍFICAS**, sendo aplicáveis somente os regramentos gerais definidos no subitem anterior.
		B) OBRIGAÇÕES ESPECÍFICAS. Indicar:
	(X)	Assinar o Termo de Confidencialidade constante do anexo deste instrumento, no qual se comprometerá a guardar os dados e as informações fornecidas, geradas e/ou de propriedade do MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA, de forma confidencial e sigilosa, vedada qualquer forma de divulgação, reprodução e/ou cessão.

3.10 OBRIGAÇÕES DO CONTRATANTE*

OBRIGAÇÕES GERAIS

3.10.1 Fornecer, no prazo de até 10 (dez) dias a contar do início da vigência da contratação, as informações necessárias para que a empresa contratada possa executar plenamente o objeto contratado;

3.10.2 Realizar os pagamentos devidos pela execução do contrato, nos termos e condições previstos neste documento;

3.10.3 Permitir o eventual acesso dos empregados autorizados da empresa contratada às instalações físicas do **MPBA**, nos locais e na forma que se façam necessários para a execução contratual;

3.10.4 Acompanhar e fiscalizar o fiel cumprimento dos prazos e das condições da contratação, notificando a empresa contratada, por escrito, sobre imperfeições, falhas ou irregularidades constatadas na execução do objeto, para que sejam adotadas as medidas corretivas necessárias;

3.10.5 Fornecer à empresa contratada, mediante solicitação, atestado de capacidade técnica, quando o fornecimento do objeto atender satisfatoriamente os prazos de entrega, qualidade e demais condições previstas em edital e seus anexos.

OBRIGAÇÕES ESPECÍFICAS (DEFINIDAS EM RAZÃO DO OBJETO CONTRATADO):

(X)	**A) NÃO EXISTEM OBRIGAÇÕES ESPECÍFICAS,** sendo aplicáveis somente os regramentos gerai definidos no subitem anterior.
( )	**B) OBRIGAÇÕES ESPECÍFICAS.** Indicar:

3.11 INDICAÇÃO SOBRE A NECESSIDADE DE GARANTIA	( )	**A) NÃO SE APLICA (CONTRATAÇÕES SEM FORMALIZAÇÃO DE CONTRATO)**
	(X)	**B) NÃO SERÁ EXIGIDA GARANTIA CONTRATUAL**

CONTRATUAL, COM PERCENTUAL ESCOLHER UMA OPÇÃO ***(Marcar com X):***	**( )**	**C) SERÁ EXIGIDA GARANTIA CONTRATUAL.** Regras: ➢ Percentual exigido: **( )** 5% (cinco por cento) **OU** **( )** Outro. Indicar: _____ % (_____ por cento) ➢ Prazo para apresentação: _____ dias após assinatura do contrato.

ANEXO I – TABELA INDICATIVA DE ITENS

1. INDICAÇÃO DOS ITENS QUE COMPÕEM O OBJETO:

1.1 DETALHAMENTO DOS ITENS

Item	Descrição (Especificações técnicas)	Unidade de Fornecimento	Quantidade	Valor unitário	Valor total por item
1	Pentest (Teste De Intrusão)	UND	1	R$ 8.202,67	R$ 8.202,67
Valor Total dos itens					R$ 8.202,67

ANEXO II – ESPECIFICAÇÕES TÉCNICAS DETALHADAS

1. **Caraterísticas Gerais:**

1.1. A atividade de Teste de Intrusão/Penetração (Pentest) deve compreender o teste de Invasão externa e tem como objetivo principal identificar, possíveis vulnerabilidades na aplicação WEB VOTO ELETRÔNICO da CONTRATANTE. Estes testes envolvem o uso de técnicas e ferramentas para tentar o acesso privilegiado aos ativos e informações da CONTRATANTE por meio de simulações controladas de ataques reais, sendo o ambiente da aplicação da CONTRATANTE avaliado em sua totalidade em busca de vulnerabilidades que possam permitir a obtenção de acesso não-autorizado, sendo que a modalidade de teste de intrusão/penetração a ser realizado será do tipo Black Box.

1.2. O teste Black Box parte da premissa que o profissional não tem informações sobre o sistema nem da estrutura da empresa e trata a aplicação como uma "caixa preta". Sendo mais difícil de ser aplicado, já que é preciso colher algumas informações para tentar explorar vulnerabilidades, mas em compensação, essa simulação fica mais próxima de um ataque real feito externamente por hackers.

1.3. A CONTRATADA deverá realizar testes de intrusão para identificação de vulnerabilidades por meio de simulações de invasão de serviços e infraestrutura (Teste de Invasão) a serem executadas externamente (através da Internet), com duração de até 30 (trinta) dias.

1.4. A CONTRATADA deverá elaborar "Relatório de Teste de Invasão" para cada teste realizado no período, apresentando todas as informações sobre o mesmo, contemplando no mínimo: objetivos, premissas e escopo do teste; metodologia de análise de vulnerabilidades; descrição das ações realizadas; vulnerabilidades encontradas; categorização e severidade das vulnerabilidades, recomendações e controles de segurança necessários para correção das vulnerabilidades; apresentação das evidências; referências e ferramentas utilizadas. Pelo período de 30 (trinta) dias, este "Relatório de Teste de Invasão" será o insumo para que a equipe técnica da CONTRATANTE possa realizar as mitigações necessárias visando sanar as vulnerabilidades o apontadas.

1.5. A Metodologia adotada pela CONTRATADA durante o Pentest deve incluir minimamente, quando pertinente, as seguintes vulnerabilidades:

1. Injeção de Código.
1. Quebra de Autenticação.
1. Exposição de Dados Sensíveis.
1. Entidades Externas de XML.
1. Quebra de Controle de Acesso.
1. Configuração Incorreta de Segurança.
1. Cross-Site Scripting (XSS).
1. Desserialização Insegura.
1. Utilização de Componentes com Vulnerabilidades Conhecidas.
1. Log e Monitoramento Ineficientes.

1.6. A CONTRATADA deverá minimamente compreender atividades que busquem encontrar vulnerabilidades em potencial, de eventual má configuração, de falhas em hardwares e softwares desconhecidos, de técnicas de contramedidas ou deficiências na infraestrutura ou sistemas da CONTRATANTE;

1.7. A CONTRATANTE deve criar um usuário interno para a CONTRATADA no ambiente da CONTRATANTE com todas suas ações logadas para documentação e atestar a integridade do trabalho realizado pela CONTRATADA.
1.8. O alvo do PENTEST (Teste de Invasão) será a aplicação aqui denominada VOTO ELETRÔNICO. Todas as fases dos PENTEST poderão ser acompanhadas e supervisionadas a qualquer momento pelo CONTRATANTE. Quaisquer atividades com suspeita de comprometimento de algum ambiente ou ativo, deverá a CONTRATADA ser reportada pelo CONTRATANTE;
1.9. Os serviços contratados deverão ser obrigatoriamente executados de fora das dependências da CONTRATANTE, simulando o quanto possível um ataque real, conforme modelo Blackbox do pentest solicitado.

1.10. O teste de penetração deverá incluir ,no mínimo, as seguintes técnicas de teste:
1. Ping sweep de intervalos de redes;
1. Verificação de portas de hosts de destino;
1. Verificação de vulnerabilidades dos alvos;
1. Penetração em alvos;
1. Manipulação no nível do aplicativo;
1. Engenharia reversa Java / ActiveX do lado do cliente;
1. Ataques de negação de serviço;
1. Verificações / explorações perigosas.

2. COMPROVAÇÃO DAS CARACTERÍSTICAS TÉCNICAS

2.1. O não atendimento às especificações técnicas descritas neste EDITAL implicará a desclassificação da proposta apresentada.
2.2. A comprovação do atendimento às características técnicas especificadas neste EDITAL dar-se-á por meio da apresentação de um ou mais casos de sucesso fornecidos por pessoas jurídicas de direito público ou privado e de comprovação de equipe técnica capacitada para execução de atividade pertinente e compatível em características, quantidades e prazos com o objeto da licitação.
2.3. No momento da assinatura do contrato a CONTRATADA deverá apresentar a lista de profissionais, com suas devidas certificações, que irão atuar no Pentest (testes de intrusão/penetração).
2.4. A prestação do Serviço de Teste de intrusão deverá ser realizada por empresa que atenda os seguintes critérios mínimos:
2. Certificação Ethical Hacking Foundation
2. Certificação ISO 27001
2. Equipe de Ethical Hackers com acesso à Deep e Dark para consultar e entender as principais técnicas que vêm sendo utilizadas por hackers ao redor do mundo.
2. Empresa possuir equipes de Blue Team e Red Team.
2. Empresa possuir caso de sucesso de suporte à recuperação de ataques cibernéticos.
2. Empresa possuir pelo menos 3 anos de funcionamento.
2. Empresa possuir pelo menos 01 atestado técnico de serviços de segurança da informação.

2.5. Os Documentos poderão ser apresentados em original, cópia autenticada ou cópia simples acompanhada do original para conferência pela Comissão.
2.6. As propostas serão analisadas por equipe de técnicos da CONTRATANTE para fins de verificação do atendimento às características da solução especificados neste EDITAL.

2.7. A falta de informações técnicas ou a incompatibilidade destas com as características especificadas implicará a desclassificação da proposta.

3. SIGILO E INVIOLABILIDADE

3.1. A CONTRATADA compromete-se a manter em caráter confidencial as informações abaixo mencionadas, mesmo após a eventual rescisão do contrato:

3. Política de segurança adotada pelo CONTRATANTE e configurações de hardware e software decorrentes;
3. Processo de instalação, configuração e customizações de produtos, ferramentas e equipamentos e atendimento aos itens de segurança, constantes do Edital de licitação;
3. Processo de implantação no ambiente do CONTRATANTE, de mecanismos de criptografia e autenticação utilizados;
3. Recomendações e implementações decorrentes do processo de consultoria;
3. Quaisquer dados que a CONTRATADA venha a ter conhecimento em decorrência da presente contratação, pertinentes a hardware, serviços e sistemas aplicativos do CONTRATANTE, cujo conhecimento por terceiros exponha o ambiente a riscos de invasão ou resulte na vulnerabilidade do mesmo.
3. Não fazer uso das informações prestadas pela CONTRATANTE que não seja em absoluto cumprimento ao contrato em questão.
3. A quebra da confidencialidade ou sigilo de informações obtidas na prestação de serviços ensejará multa, responsabilidade criminal na forma da lei, sem prejuízo de outras providências nas demais esferas. A CONTRATADA obriga-se a tomar as providências necessárias para assegurar que as informações confidenciais não sejam divulgadas por seus empregados ou agentes.

MINISTÉRIO PÚBLICO
DO ESTADO DA BAHIA

DESPACHO

Retorne-se o presente expediente à Diretoria de Contratos e Licitações informando que as respostas solicitadas estão no corpo do despacho.

2. Sugerimos que, no formulário "Dispensa de Licitação - Formulário de Autorização/Solicitação", sejam informados os nomes e valores dos itens conforme ordem decrescente de preços, de modo que o fornecedor 1 seja aquele que apresentou o valor mais baixo para a contratação pretendida.

R. Estaremos atentos, nos próximos processos desta sugestão. Sugerimos que coloquem esta solicitação em algum dos documentos de passo a passo, pois não achamos em nenhum deles esta informação.

3. Verificamos que na Procuração constante no procedimento (0169642) Maria Magali Bredariol, cujo documento de identidade se encontra no expediente (0165289), tem poderes outrogados apenas pela empresa ORBITALL ATENDIMENTO LTDA. Além da referida outrorgante não ser a empresa indicada como contratada, a supracitada Procuradora somente poderia agir em conjunto com um Diretor ou com outro Procurador devidamente constituído no que diz respeito à representação da empresa em contratações com pessoas físicas ou jurídicas.

R. Segue abaixo o e-mail da empresa em relação ao questionamento, ainda assim anexamos como documento anexo(0180214)

De: Patricia Goncalves Maia Dantas <pmdantas@stefanini.com>
Enviado: sexta-feira, 13 de agosto de 2021 09:54
Para: Iaçanã Lima de Jesus Carneiro <iassa@mpba.mp.br>
Assunto: ENC: Questionamento da área de Contratos do MPBA

Iaçanã,

Para otimizar a procuração, Marco e Graça fizeram uma procuração contendo várias empresas do grupo da qual eles são sócios e deram poderes para assinar para a Magali. A Stefanini Rafael é o item 3 da procuração.

PROCURAÇÃO BASTANTE QUE FAZ: ORBITALLSERVIÇOS E PROCESSAMENTO DE MEIOS DEPAGAMENTO LTDA e outros

SAIBAM quantos este público instrumento de procuração bastante virem que, aos trinta e um (31) dias do mês de maio do ano de dois mil e vinte e um (2021), neste Oficial do Registro Civil das Pessoas Naturais do 39º Subdistrito Vila

Madalena, por vídeo conferência nos termos do Provimento 100 do CNJ, perante mim, SUBSTITUTA, compareceram como outorgantes:

[...]

3) STEFANINI RAFAEL SEGURANÇA E DEFESA S.A., sociedade anônima,

inscrita no CNPJ/MF de nº 24.691.488/0001-09, com sede na Avenida Eusébio Matoso, 1375, 8º andar, salas 801 e 802, Butantã, CEP 05423-905, São Paulo, SP, com seu Estatuto Social Consolidado, anexo a Ata da Assembleia Geral Extraordinária, realizada aos 09/01/2017, devidamente registrada na Junta Comercial do Estado de São Paulo (JUCESP) aos 24/02/2017, sob nº 106.436/17-0 e Certidão Simplificada Eletrônica, emitida pela Junta

supramencionada, aos 16/04/2021, autenticidade nº 150428367, neste ato representada nos termos dos ARTIGOS 13, 18 - Parágrafo 1º, 19 - Parágrafo 1º, do documento supracitado, cuja cópia fica arquivada nesta Serventia em Pasta Própria (CS 70, fls. 58), pelos Diretores eleitos conforme Instrumento Particular de 1ª Alteração ao Contrato Social e Assembleia Geral de Transformação, datado de 10/05/2016, devidamente registrado na Junta Comercial do Estado de São Paulo (JUCESP), aos 24/06/2016, sob nº 3530049265-0: MARCO ANTONIO SILVA STEFANINI, brasileiro, casado, empresário, portador da cédula de identidade RG nº 10.153.181-3 SSP/SP, inscrito no CPF/MF sob nº 042.501.968-36, residente e domiciliado na Rua Marcos Melega, 150 - 3H, Edifício Casuarina - Alto de Pinheiros, São Paulo SP, CEP 05466-010, MARIA DAS GRAÇAS VUOLO SAJOVIC STEFANINI, brasileira, casada, empresária, portadora da cédula de identidade RG nº 8.546.223-8 SSP/SP, inscrita no CPF/MF sob nº 15.819.138-26, residente e domiciliada na Rua Marcos Melega, 150 - 3H, Edifício Casuarina, Alto de Pinheiros, São Paulo SP, CEP 05466-010;

Se precisarem de qualquer complemento de informação favor entrar em contato.

PATRÍCIA MAIA DANTAS
DIRETORA NEGÓCIOS - GOVERNO

-
+ 55 71 99624-7432

WWW.STEFANINI.COM

No Documento de Oficialização da Demanda:

4. No item 2.3 e 2.4 do Anexo ao DOD, informa-se que a Contratada permanecerá, durante todo o prazo de execução, qual seja, 30 dias, realizando diversos testes. Compreendemos, dete modo, que os serviços serão realizados de maneira contínua, dentro do prazo de execução dos mesmos, com entregas periódicas de relatórios dos testes realizados. Neste sentido, e considerando que havia previsão na contratação anterior, conforme indicado abaixo, solicitamos esclarecimento acerca da necessidade ou não de definição de prazos para entregas periódicas dos relatórios de teste de invasão.

R. Entendemos que devem estar se referindo aos itens 1.3 e 1.4 e não aos 2.3 e 2.4, que tratam de assunto diverso ao exposto no questionamento.

Não há necessidade de definição de prazos entre as entregas dos relatórios preliminares, pois é da natureza do serviço que ocorram re testes, pois se necessita realizar as mitigações ao longo do processo até a data final da contratação, momento em que se espera que todas as necessidade de mitigação tenha sido devidamente realizadas.

5. O item 3.2.5 do Documento de Oficialização da Demanda conflita com a informação constante do item 2.9 do Anexo do mencionado documento. Faz-se necessário compatibilizar tais informações.

R. Item alterado conforme indicado no DOD.

***6.** O tópico 3 do anexo do Documento de Oficialização da Demanda indica informações a serem prestadas como condição de habilitação de empresa em procedimento licitatório. Tratando-se de procedimento de contratação por Dispensa de Licitação, sugerimos que a área verifique, no caso concreto, se a empresa selecionada já atende àqueles critérios, anexando as respectivas comprovações no procedimento e revisando a redação do tópico de modo a indicar que aquelas características já se encontram comprovada no procedimento.*

R. Observação atendida. Os documentos foram anexados ao processo.

7. Considerando que as informações constantes no tópico 4 do anexo do Documento de Oficialização da Demanda já constam no item 3.9 do referido documento, sugerimos que o tópico do anexo seja excluído. Ademais, sugerimos a adequação da redação do item 3.9, de modo a indicar que a obrigação da contratada é de assinar o Termo de Confidencialidade e que este documento deverá conter as informações ali dispostas.

R. Pecamos pelo excesso, pois o fornecedor recebe a especificação técnica e não o DOD, motivo pelo qual constou o item duplicado no documento.

Acatamos a sugestão sobre requerer apenas a assinatura do Termo de Confidencialidade contendo todos os requisitos. DOD alterado e anexado.

Informações não encontradas no DOD, porém constantes na contratação anteriormente realizada:

8. Relativamente ao recebimento e/ou condição de pagamento (Itens 3.4 e 3.6): "A entrega do Relatório de testes é indispensável ao recebimento do objeto deste instrumento, nos termos definidos neste instrumento". Neste sentido, sugerimos tal previsão até mesmo para viabilizar a entrega do último relatório ao recebimento dos serviços executados (e consequentemente melhor documentar a habilitação para pagamento do fornecedor).

R. Acatada sugestão. Acrescentado o texto no sub item 3.6.3.7, do item 3.6

9. *Relativamente às obrigações da Contratada (Item 3.9): "Acompanhar e informar sobre as atualizações tecnológicas necessárias para executar os serviços adquiridos, realizando as ações necessárias para a implantação dessas atualizações em comum acordo com o CONTRATANTE, até o final do contrato, sem ônus para o CONTRATANTE".*

R. **Acatamos a sugestão da redação. Incluído o sub item 3.9.1.6 do item 3.9**

Sugestões de melhoria:

10. *Sugerimos adequar a redação do item 2.6 do anexo do DOD de modo a evidenciar que as atividades da contratada deverão compreender o conjunto de atividades informado, além de excluir a expressão "DOCUMENTO DE OFICIALIZAÇÃO DA DEMANDA SERVIÇOS DISPENSA" no final do texto. Propomos a seguinte redação (a ser analisada em sua conformidade pela Unidade demandante): "A CONTRATADA deverá desenvolver atividades que, minimamente, busquem encontrar vulnerabilidades em potencial, de eventual má configuração, de falhas em hardwares e softwares desconhecidos, de técnicas de contramedidas ou deficiências na infraestrutura ou sistemas do CONTRATANTE".*

R. **Acreditamos que o item mencionado se trata do 1.6 invés do 2.6. Não encontramos a menção no fim do texto "Documento de Oficialização da Demanda"**

Agradecemos a sugestão da redação, mas iremos manter o que já está escrito e que foi devidamente entendido por todos os que participaram desta dispensa de licitação.

Documento assinado eletronicamente por **Iaçanã Lima de Jesus Carneiro** em 05/58/05021, s 2às 01con:orme art42f1...1º1da " ei 224b2L/05564

A autenticidade do documento pode ser con:erida no site https9/sei4sistemas4mpl a4mp4 r/sei/controlador_externo4php?acao=documento_con:erir&id_orgao_acesso_externo=5 in:ormando o código veri:icador **0180216** e o código CRC **1FB4378F**4

MINISTÉRIO PÚBLICO
DO ESTADO DA BAHIA

MANIFESTAÇÃO

Informamos que o despacho da DCCL foi devidamente respondido.

Documento assinado eletronicamente por **Iaçanã Lima de Jesus Carneiro** em 02/28/0201, às 19:23, conforme art. 1º, III, "b", da Lei 11.416/0229.

A autenticidade do documento pode ser conferida no site https://sei.sistemas.mpba.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=2 informando o código verificador **0180240** e o código CRC **C23E0684**.

MINISTÉRIO PÚBLICO
DO ESTADO DA BAHIA

DESPACHO

Encaminhamos o presente expediente contendo a proposta de minuta do contrato para fins de aprovação por esta Diretoria.

Ressaltamos que, caso se identifique a necessidade de modificação do seu teor, esta unidade indique os ajustes a serem realizados através de manifestação inserida neste procedimento, devolvendo-o, em seguida, a esta Coordenação para readequação da minuta.

Após aprovação ou eventuais ajustes necessários, encaminharemos o processo à Assessoria Técnico-Jurídica para análise e manifestação.

Documento assinado eletronicamente por **Mariana Nascimento Sotero Campos** em 03/09/2021, às 13:14, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.sistemas.mpba.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0188917** e o código CRC **8352D9DD**.

MINISTÉRIO PÚBLICO
DO ESTADO DA BAHIA

CONTRATO PARA PRESTAÇÃO DE SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO, QUE ENTRE SI CELEBRAM O MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA E A EMPRESA STEFANINI RAFAEL SEGURANÇA E DEFESA S.A, NA FORMA ABAIXO:

CONTRATO Nº xxx/2021 - SGA

O **MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA**, CNPJ nº 04.142.491/0001-66, com sede situada à 5ª Avenida, 750, Centro Administrativo da Bahia - CAB, Salvador - BA, neste ato representado, mediante Ato de Delegação nº 70/2014, pelo Superintendente de Gestão Administrativa **Frederico Welington Silveira Soares**, doravante denominado **CONTRATANTE**, e a **EMPRESA STEFANINI RAFAEL SEGURANÇA E DEFESA S.A.**, CNPJ nº 24.691.488/0001-09, estabelecida à Avenida Eusebio Matoso, nº 1375, Andar 8, Salas 801 e 802, Butantã, CEP 05423-905, São Paulo/SP, representada por sua **representante legal,** Sra. **Maria Magali Bredariol,** inscrito no CPF/MF nº 437.349.448-72, doravante denominada **CONTRATADA**, com supedâneo no quanto disposto na Lei Estadual-BA nº 9.433/2005, na Medida Provisória nº 961 de maio de 2020, e, ainda, observado o constante no processo de Dispensa de Licitação nº 004/2021-DTI protocolado sob o nº 19.09.02684.0011790/2021-22, o qual integra este instrumento independentemente de transcrição, **CELEBRAM** o presente Contrato, mediante as cláusulas e condições seguintes:

CLÁUSULA PRIMEIRA - DO OBJETO

1.1 Constitui objeto do presente contrato a prestação de serviços técnicos, na área de tecnologia da informação, para a varredura de vulnerabilidades e testes de intrusão – PENTEST – na aplicação WEB VOTO DIGITAL, no formato Black Box, nos termos e condições do presente instrumento.

CLÁUSULA SEGUNDA – DO REGIME DE EXECUÇÃO, DA ENTREGA E DO RECEBIMENTO

2.1 O regime de execução do contrato é o de Empreitada Indireta por preço global;

2.2 O **CONTRATANTE** convocará a **CONTRATADA** para retirar a nota de empenho no prazo de até 05 (cinco) dias contados da data da notificação, a ser efetivada, preferencialmente, por e-mail;

Anexo Proposta de Minuta de Contrato (0188921) SEI 19.09.02684.0011790/2021-22 / pg. 626

2.2.1 As comprovações da convocação e da entrega/retirada da nota de empenho poderão ocorrer por quaisquer dos seguintes meios: por meio eletrônico (através de confirmação de recebimento de e-mail), aposição de assinatura (para retirada presencial) ou por Aviso de Recebimento dos correios (quando a entrega for via postal).

2.2.2 A **CONTRATADA** poderá solicitar a prorrogação do prazo para retirada/recebimento da nota de empenho, por igual período ao original, por motivo justo e aceito pela Administração, nos termos do art. 124, § 4º, da Lei Estadual – BA nº 9433/2005.

2.3 O Teste de Intrusão/Penetração (PENTEST) compreende o teste de Invasão externa e tem como objetivo principal identificar, possíveis vulnerabilidades na aplicação WEB VOTO DIGITAL da **CONTRATANTE**, observando-se ainda:

2.3.1 Os serviços objeto deste instrumento envolvem o uso de técnicas e ferramentas para tentar o acesso privilegiado aos ativos e informações do **CONTRATANTE** por meio de simulações controladas de ataques reais, sendo o ambiente da aplicação do **CONTRATANTE** avaliado em sua totalidade em busca de vulnerabilidades que possam permitir a obtenção de acesso não-autorizado, sendo que a modalidade de teste de intrusão/ penetração a ser realizado será do tipo Black Box;

2.3.2 A **CONTRATADA** deverá realizar testes de intrusão para identificação de vulnerabilidades por meio de simulações de invasão de serviços e infraestrutura (Teste de Invasão) a serem executadas externamente (através da Internet);

2.3.3 A **CONTRATADA** deverá minimamente compreender atividades que busquem encontrar vulnerabilidades em potencial, de eventual má configuração, de falhas em hardwares e softwares desconhecidos, de técnicas de contramedidas ou deficiências na infraestrutura ou sistemas da **CONTRATANTE**;

2.3.4 O **CONTRATANTE** deve criar um usuário interno para a **CONTRATADA** no ambiente da **CONTRATANTE** com todas suas ações logadas para documentação e para atestar a integridade do trabalho realizado pela **CONTRATADA**.

2.4 A **CONTRATADA** deverá elaborar "Relatório de Teste de Invasão" para cada teste realizado no período, apresentando todas as informações sobre o mesmo, contemplando no mínimo: objetivos, premissas e escopo do teste; metodologia de análise de vulnerabilidades; descrição das ações realizadas; vulnerabilidades encontradas; categorização e severidade das vulnerabilidades, recomendações e controles de segurança necessários para correção das vulnerabilidades; apresentação das evidências; referências e ferramentas utilizadas.

2.4.1 Pelo período de 30 (trinta) dias, ou seja, durante todo o prazo de execução, este "Relatório de Teste de Invasão" será o insumo para que a equipe técnica da **CONTRATANTE** possa realizar as mitigações necessárias visando sanar as vulnerabilidades o apontadas.

2.4.2 A **CONTRATADA** deverá apresentar o relatório de vulnerabilidades encontradas e mitigadas em reunião por vídeo conferência com a Diretória de Tecnologia - DTI do **CONTRATANTE**, bem como enviá-lo para o e-mail casi@mpba.mp.br, respeitando-se o prazo de execução definido no **item 2.6**.

2.5 Todas as fases dos PENTEST poderão ser acompanhadas e supervisionadas a qualquer momento pela equipe técnica do **CONTRATANTE**;

2.5.1 A **CONTRATADA** deverá reportar ao **CONTRATANTE** quaisquer atividades com suspeita de comprometimento de algum ambiente ou ativo;

2.5.2 O teste de penetração (PENTEST) incluirá, no mínimo, as seguintes técnicas de teste:

2.5.2.1 Ping sweep de intervalos de redes;

2.5.2.2 Verificação de portas de hosts de destino;

2.5.2.3 Verificação de vulnerabilidades dos alvos;

2.5.2.4 Penetração em alvos;

2.5.2.5 Manipulação no nível do aplicativo;

2.5.2.6 Engenharia reversa Java / ActiveX do lado do cliente;

2.5.2.7 Ataques de negação de serviço;

2.5.2.8 Verificações / explorações perigosas.

2.5.3 A metodologia adotada pela **CONTRATADA** durante o PENTEST deve incluir, minimamente, quando pertinente, as seguintes vulnerabilidades:

2.5.3.1 Injeção de Código;

2.5.3.2 Quebra de Autenticação;

2.5.3.3 Exposição de Dados Sensíveis;

2.5.3.4 Entidades Externas de XML;

2.5.3.5 Quebra de Controle de Acesso;

2.5.3.6 Configuração Incorreta de Segurança;

2.5.3.7 Cross-Site Scripiting (XSS);

2.5.3.8 Desserialização Insegura;

2.5.3.9 Utilização de Componentes com Vulnerabilidades Conhecidas;

2.5.3.10 Log e Monitoramento Ineficientes;

2.6 O prazo para execução dos serviços é de 30 (trinta) dias, contados da data da entrega à **CONTRATADA**, da nota de empenho, acompanhada, se for o caso, da autorização de serviços, e do instrumento contratual;

2.6.1 O prazo de execução poderá ser prorrogado por mais 30 (trinta) dias, desde que seja formalmente solicitado pela **CONTRATADA** antes do termo final do prazo de entrega consignado, mediante justificativa e respectiva comprovação de fato superveniente, aceito pela Instituição.

2.7 Os serviços objeto deste contrato deverão ser executados por profissionais que possuam capacitação técnica compatível com as atividades que lhes forem incumbidas, sob inteira responsabilidade da **CONTRATADA**, que deve orientar os mesmos quanto às suas obrigações e afazeres;

2.8 Os serviços contratados deverão ser obrigatoriamente executados fora das dependências da **CONTRATANTE**, simulando o quanto possível um ataque real, conforme modelo Black Box do PENTEST solicitado.

2.9 O recebimento dos serviços prestados ficará sob a responsabilidade de um representante da Diretoria de Tecnologia da Informação do **CONTRATANTE**, em conjunto com o fiscal do contrato - responsável pela habilitação para pagamentos, caso este não seja integrante daquela Diretoria;

2.9.1 A entrega do Relatório de testes é indispensável ao recebimento do objeto deste instrumento, nos termos definidos no **item 2.4**;

2.9.2 O recebimento provisório se dará no prazo de 05 (cinco) dias, contados da entrega do relatório final de testes;

2.9.3 O **CONTRATANTE** rejeitará, no todo ou em parte, o objeto contratual em desacordo com as condições pactuadas, podendo, entretanto, se lhe convier, decidir pelo recebimento, neste caso com as deduções cabíveis;

2.10 O recebimento definitivo do objeto deste contrato se dará no prazo de 10 (dez) dias, contados da entrega do relatório final de testes, e será concretizado depois de adotados, pelo **CONTRATANTE**, todos os procedimentos contidos nos Ato Normativos internos relativos ao tema, respeitadas as exigências contidas do art. 161 da Lei Estadual- BA nº 9.433/2005;

2.11 O aceite ou aprovação do objeto pelo **CONTRATANTE** não exclui a responsabilidade da **CONTRATADA** por vícios, defeitos ou disparidades com as especificações estabelecidas neste Contrato e no processo de Licitação que o originou, verificadas posteriormente, garantindo-se ao **CONTRATANTE**, inclusive, as faculdades previstas na Lei Federal nº 8.078/90 – Código de Defesa do Consumidor.

CLÁUSULA TERCEIRA - DA DOTAÇÃO ORÇAMENTÁRIA

As despesas para o pagamento deste contrato correrão por conta da Dotação Orçamentária a seguir especificada:

Código Unidade Orçamentária/Gestora	**Ação (P/A/OE)**	**Região**	**Destinação de Recursos (Fonte)**	**Natureza da Despesa**
40.601/0003	2002	9900	0100	33.90.40

CLÁUSULA QUARTA - DO PREÇO

4.1 Dá-se ao presente Contrato o valor global de R$ 8.202,67 (oito mil, duzentos e dois reais e sessenta e sete centavos);

4.2 Nos preços computados neste Contrato estão inclusos todos e quaisquer custos necessários ao fiel cumprimento deste instrumento, inclusive todos aqueles relativos a remunerações, encargos sociais, previdenciários e trabalhistas de todo o pessoal disponibilizado pela **CONTRATADA** para a execução do objeto, materiais empregados, aluguéis, licenças, administração, tributos e emolumentos.

Anexo Proposta de Minuta de Contrato (0188921) SEI 19.09.02684.0011790/2021-22 / pg. 630

CLÁUSULA QUINTA – DOS ACRÉSCIMOS E DAS SUPRESSÕES

5.1 A **CONTRATADA** se obriga a aceitar, quando solicitado e devidamente motivado pela Administração, nas mesmas condições estabelecidas neste instrumento, os acréscimos ou supressões de até 25% (vinte e cinco por cento) do valor inicial atualizado do contrato, na forma da Lei Estadual - BA nº 9.433/2005;

5.2 As supressões poderão ser superiores a 25% (vinte e cinco por cento), desde que haja resultado de acordo entre os contratantes.

CLÁUSULA SEXTA - DAS CONDIÇÕES DO PAGAMENTO E DA RETENÇÃO DOS TRIBUTOS

6.1 O pagamento dos serviços objeto deste instrumento será processado em parcela única, após a realização dos serviços, mediante apresentação, pela **CONTRATADA**, de Nota Fiscal e demais documentos/certidões cabíveis, documentação que deverá estar devidamente acompanhada do **TERMO DE ACEITE** do objeto pelo **CONTRATANTE;**

6.1.1 O pagamento se concluirá no prazo de 08 (oito) dias úteis a contar da data de apresentação da documentação (com respectivo aceite), desde que não haja pendência a ser regularizada;

6.1.2 Verificando-se qualquer pendência impeditiva do pagamento, será considerada como data de apresentação da documentação aquela na qual foi realizada a respectiva regularização;

6.2 As notas fiscais/faturas far-se-ão acompanhar da documentação probatória relativa ao recolhimento dos tributos, que tenham como fato gerador o objeto consignado na **CLÁUSULA PRIMEIRA**;

6.3 O **CONTRATANTE** realizará a retenção de impostos ou outras obrigações de natureza tributária, na hipótese de figurar como substituto tributário, de acordo com a legislação vigente;

6.4 Os pagamentos serão efetuados através de ordem bancária, para crédito em conta corrente e agência indicadas pela **CONTRATADA**, preferencialmente em banco de movimentação oficial de recursos do Estado da Bahia;

6.5 A atualização monetária dos pagamentos devidos pelo **CONTRATANTE**, em caso de mora, será calculada considerando a data do vencimento da obrigação e do seu efetivo pagamento, de acordo com a variação do INPC do IBGE *pro rata tempore,* observado, sempre, o disposto no item 6.1 e

seus subitens.

6.5.1 Para efeito de caracterização de mora imputável ao **CONTRATANTE**, não serão considerados eventuais atrasos de pagamento no período de fechamento do exercício financeiro do Estado da Bahia, compreendido entre o final do mês de dezembro e o mês de janeiro do exercício subsequente, decorrentes de circunstâncias alheias à vontade das partes, isto é, por força de bloqueio de rotinas no sistema estadual obrigatoriamente utilizado para a execução dos pagamentos devidos pelo **CONTRATANTE**.

CLÁUSULA SÉTIMA – DO REAJUSTAMENTO E DA REVISÃO DE PREÇOS

7.1 O preço definido na **CLÁUSULA QUARTA** é irreajustável;

7.2 A revisão de preços nos termos do inc. XXVI do art. 8º da Lei Estadual nº. 9.433/2005, por interesse da **CONTRATADA**, dependerá de requerimento formal, instruído com a documentação que comprove o desequilíbrio econômico-financeiro do Contrato. Deverá ser instaurada pelo **CONTRATANTE**, entretanto, quando este pretender recompor o preço que se tornou excessivo.

7.2.1 A revisão de preços, se ocorrer, deverá ser formalizada através de celebração de Aditivo Contratual.

CLÁUSULA OITAVA – DA VIGÊNCIA

O prazo de vigência do presente Contrato será de 90 (noventa) dias, contados da data da sua publicidade no Diário de Justiça Eletrônico (DJ-e) do Poder Judiciário do Estado da Bahia, podendo ser prorrogado, mediante termo aditivo e após manifestação da autoridade competente.

CLÁUSULA NONA – DAS OBRIGAÇÕES DA CONTRATADA

9.0 Além das determinações contidas no procedimento que originou esta contratação – que aqui se consideram literalmente transcritas, bem como daquelas decorrentes de lei, a **CONTRATADA,** obriga-se a:

9.1 Promover a execução contratual de acordo com as especificações técnicas e exigências constantes no presente contrato e no procedimento administrativo que o originou, conforme dias, horários e prazos contratados, não podendo eximir-se da obrigação, ainda que parcialmente, sob a alegação de falhas, defeitos ou falta de rede, sistema, pessoal, peça e/ou material;

9.2 Manter sob sua exclusiva responsabilidade toda a supervisão e direção da mão de obra necessária para execução completa e eficiente dos serviços objeto deste contrato;

9.3 Prestar diretamente os serviços ora contratados, não os transferindo a outrem, no todo ou em parte, ressalvando-se apenas os casos de cisão, fusão ou incorporação da **CONTRATADA**, desde que não impeçam os compromissos pautados neste instrumento contratual, ficando vedada a subcontratação, ainda que parcial, dos serviços que compõem o objeto deste instrumento;

9.4 Acompanhar e informar sobre as atualizações tecnológicas necessárias para executar os serviços adquiridos, realizando as ações necessárias para a implantação dessas atualizações em comum acordo com o **CONTRATANTE**, até o final do contrato, sem ônus para o **CONTRATANTE;**

9.5 Manter durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas para a contratação;

9.6 Responsabilizar-se pelo cumprimento das exigências previstas na legislação profissional específica e pelos encargos fiscais e comerciais resultantes da execução do contrato;

9.7 A eventual retenção de tributos pelo **MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA** não implicará na responsabilização deste, em hipótese alguma, por quaisquer penalidades ou gravames futuros, decorrentes de inadimplemento(s) de tributos pela **CONTRATADA**;

9.8 Emitir notas fiscais/faturas de acordo com a legislação, contendo descrição dos serviços, indicação de quantidades, preços unitários e valor total;

9.9 Arcar, quando da execução do objeto contratual, com todo e qualquer dano ou prejuízo, independentemente da natureza, causado ao **MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA** e/ou a terceiros, ainda que por sua culpa, em consequência de erros, imperícia própria ou de auxiliares que estejam sob sua responsabilidade, bem como ressarcir ao MPBA todos os custos decorrentes de indevida paralisação ou interrupção dos serviços contratados;

9.10 Providenciar e manter atualizadas todas as licenças e alvarás junto às repartições competentes que, porventura, sejam necessários à execução do contrato;

9.11 Não introduzir, seja a que título for, nenhuma modificação na especificação do objeto contratado, sem o consentimento prévio, e por escrito, do **MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA**;

9.12 Atender, nos prazos consignados neste instrumento, às recusas ou determinações, pelo **MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA**, de realização/refazimento de serviços que não estejam sendo ou não tenham sido executados de acordo com as Normas Técnicas e/ou em conformidade com as condições deste contrato ou do procedimento que o originou, providenciando sua correção ou realização, sem ônus para o **MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA**;

9.13 Permitir e oferecer condições para a mais ampla e completa fiscalização durante a vigência deste contrato, fornecendo informações, propiciando o acesso à documentação pertinente e à execução contratual, e atendendo às observações e exigências apresentadas pela fiscalização;

9.14 Comunicar formalmente ao **MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA** qualquer anormalidade que interfira no bom andamento da execução do Contrato;

9.15 Prestar todos os esclarecimentos que forem solicitados pelo **MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA**, durante a vigência deste instrumento;

9.16 Assinar o Termo de Confidencialidade constante do **Anexo I** deste instrumento, no qual se comprometerá a guardar os dados e as informações fornecidas, geradas e/ou de propriedade do **MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA**, de forma confidencial e sigilosa, vedada qualquer forma de divulgação, reprodução e/ou cessão.

CLÁUSULA DÉCIMA – DAS OBRIGAÇÕES DO CONTRATANTE

10 O **CONTRATANTE,** além das obrigações contidas neste contrato por determinação legal, obriga-se a:

10.1 Fornecer, no prazo de 10 (dez) dias a contar da data da publicação do contrato, as informações necessárias para que a **CONTRATADA** possa executar plenamente o objeto contratado;

10.2 Realizar os pagamentos devidos pela execução do contrato, nos termos e condições previstos nas **CLÁUSULAS QUARTA e SEXTA**;

10.3 Viabilizar, no que for cabível, as condições de execução dos serviços pela **CONTRATADA**, prestando-lhe todas as informações necessárias;

10.4 Acompanhar e fiscalizar o fiel cumprimento dos prazos e das condições de realização do presente contrato, notificando a **CONTRATADA**, por escrito, sobre imperfeições, falhas ou irregularidades constatadas na execução do objeto, para que sejam adotadas as medidas corretivas necessárias;

10.5 Fornecer à **CONTRATADA**, mediante solicitação, atestado de capacidade técnica, quando o fornecimento do objeto atender satisfatoriamente os prazos de entrega, qualidade e demais condições previstas neste Contrato.

CLÁUSULA DÉCIMA PRIMEIRA – DA FISCALIZAÇÃO DO CONTRATO

11.1 Na forma das disposições estabelecidas na Lei Estadual-BA nº 9.433/2005, o **CONTRATANTE** designará servidor(es), **por meio de Portaria específica para tal fim**, para a fiscalização deste contrato, tendo poderes, entre outros, para notificar a **CONTRATADA** sobre as irregularidades ou falhas que porventura venham a ser encontradas na execução deste instrumento;

11.2 Incumbe à fiscalização acompanhar e verificar a perfeita execução do contrato, em todas as suas fases, competindo-lhe, primordialmente:

11.2.1 Acompanhar o cumprimento deste instrumento e determinar as providências necessárias à correção de falhas, irregularidades e/ou defeitos, podendo ainda suspender-lhes a execução, sem prejuízos das sanções contratuais legais;

11.2.2 Transmitir à **CONTRATADA** instruções, e comunicar alterações de prazos, cronogramas de execução e especificações do projeto, quando for o caso;

11.2.3 Promover a verificação do fornecimento efetuado, emitindo a competente habilitação para o recebimento de pagamentos;

Anexo Proposta de Minuta de Contrato (0188921) SEI 19.09.02684.0011790/2021-22 / pg. 635

11.2.4 Esclarecer as dúvidas da **CONTRATADA**, solicitando ao setor competente do **CONTRATANTE**, se necessário, parecer de especialistas;

11.3 A fiscalização, pelo **CONTRATANTE**, não desobriga a **CONTRATADA** de sua responsabilidade quanto à perfeita execução do objeto contratual;

11.3.1 A ausência de comunicação, por parte do **CONTRATANTE**, sobre irregularidades ou falhas, não exime a **CONTRATADA** das responsabilidades determinadas neste contrato;

11.4 O **CONTRATANTE** poderá recusar, sustar e/ou determinar a substituição de bens ou refazimento de serviços que não estejam sendo ou não tenham sido fornecidos ou executados de acordo com as Normas Técnicas e/ou em conformidade com as condições deste contrato ou do procedimento licitatório que o originou, ou ainda que atentem contra a segurança de terceiros ou de bens;

11.4.1 Qualquer bem ou serviço considerado não aceitável, no todo ou em parte, deverá ser refeito, reparado ou substituído pela **CONTRATADA**, às suas expensas;

11.4.2 A não aceitação de algum bem ou serviço, no todo ou em parte, não implicará na dilação do prazo de execução, salvo expressa concordância do **CONTRATANTE**;

11.5 Para fins de fiscalização, o **CONTRATANTE** poderá solicitar à **CONTRATADA**, a qualquer tempo, os documentos relacionados com a execução do presente contrato.

CLÁUSULA DÉCIMA SEGUNDA - DAS PENALIDADES

12.1 A **CONTRATADA** sujeitar-se-á às sanções administrativas previstas na Lei Estadual-BA nº. 9.433/2005, as quais poderão vir a ser aplicadas após o prévio e devido processo administrativo, assegurando-lhe, sempre, o contraditório e a ampla defesa.

12.2 - Em caso de inadimplemento parcial ou total de obrigações pela **CONTRATADA**, e não sendo suas justificativas aceitas pelo **CONTRATANTE,** àquela poderão ser aplicadas, observado o disposto no item anterior, as seguintes penalidades:

12.2.1 Multa;

Anexo Proposta de Minuta de Contrato (0188921) SEI 19.09.02684.0011790/2021-22 / pg. 636

12.2.2 Suspensão temporária de participação em licitação e impedimento de contratar com a Administração pelo prazo de até 05 (cinco) anos;

12.2.3 Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes desta punição e até que seja promovida sua reabilitação perante a Administração Pública Estadual;

12.2.4 Descredenciamento do sistema de registro cadastral.

12.3 Nas hipóteses de aplicação das sanções previstas nos **itens 12.2.2 a 12.2.4**, estas serão impostas à **CONTRATADA** cumulativamente com multa;

12.4 A inexecução contratual, inclusive por atraso injustificado na execução do contrato, sujeitará o **CONTRATADA** à multa de mora, que será que será apurada **por infração** e graduada de acordo com a gravidade da infração, obedecidos os seguintes limites máximos:

12.4.1 Para hipótese de inexecução relacionada ao cumprimento de obrigação **principal**:

12.4.1.1 - 10% (dez por cento) sobre o valor da nota de empenho ou do Contrato, em caso de descumprimento total da obrigação;
12.4.1.2 - 0,3% (três décimos por cento) ao dia, até o 30º (trigésimo) dia de atraso, sobre o valor total da parte do fornecimento ou serviço não realizado;

12.4.1.3 - 0,7% (sete décimos por cento) por cada dia de atraso subseqüente ao 30º (trigésimo), sobre o valor da parte do fornecimento ou serviço não realizado;

12.4.2 Para hipótese de inexecução relacionada ao cumprimento de obrigação **acessória**, assim consideradas aquelas que coadjuvam com a principal:

12.4.2.1 - 0,2% (dois décimos por cento) ao dia, até o 30º (trigésimo) dia de atraso, sobre o valor do contrato;

12.4.2.2 - 0,6% (seis décimos por cento) por cada dia de atraso subsequente ao 30º (trigésimo), sobre o valor do contrato;

12.4.2.3 - Para cada obrigação acessória descumprida, a aplicação dos percentuais definidos nos **subitens 12.4.2.1 e 12.4.2.2**, estará limitada ao montante global de 10% (dez por cento) do valor do contrato;

Anexo Proposta de Minuta de Contrato (0188921) SEI 19.09.02684.0011790/2021-22 / pg. 637

12.5 A aplicação de multa à **CONTRATADA** não impede que a Administração rescinda unilateralmente o contrato e aplique as demais sanções previstas na Lei Estadual-BA nº 9.433/2005;

12.6 Quando aplicadas, as multas deverão ser pagas espontaneamente no prazo máximo de 05 (cinco) dias úteis, ou serem deduzidas do pagamento a ser efetuado pelo **CONTRATANTE**, caso este deva ocorrer dentro daquele prazo;

12.6.1 Na hipótese de ausência de adimplemento voluntário e impossibilidade de dedução, as multas poderão ser cobradas judicialmente, a critério do **CONTRATANTE**;

12.7 A aplicação de multas não tem caráter compensatório, e o seu pagamento não eximirá a **CONTRATADA** da responsabilidade por perdas e/ou danos decorrentes das infrações cometidas;

12.8 Os custos correspondentes a danos e/ou prejuízos causados por culpa ou dolo da **CONTRATADA** deverão ser ressarcidos ao **CONTRATANTE** no prazo máximo de 05 (cinco) dias úteis, contados da notificação administrativa, sob pena de, sem prejuízo do ressarcimento, serem considerados como hipótese de inadimplemento contratual, sujeita, portanto, à aplicação das sanções administrativas previstas nesta Cláusula.

CLÁUSULA DÉCIMA TERCEIRA – DA RESCISÃO

13.1 A inexecução total ou parcial do Contrato ensejará a sua rescisão, com as consequências contratuais previstas no Capítulo IX, Seção VIII - Da Inexecução e da Rescisão dos Contratos, da Lei Estadual-BA nº 9.433/2005;

13.2 O **CONTRATANTE** poderá rescindir unilateral e administrativamente o presente Contrato, nas hipóteses previstas nos incisos I a XVI, XX e XXI do art. 167 da Lei Estadual-BA nº 9.433/2005;

13.3 Havendo rescisão administrativa do presente contrato, baseada em alguma das hipóteses previstas nos incisos II a XII do art. 167 da Lei Estadual-BA nº 9.433/2005, o **CONTRATANTE** poderá adotar, no que couber, quaisquer das medidas discriminadas no art. 169 do supracitado diploma legal.

CLÁUSULA DÉCIMA QUARTA – DA VINCULAÇÃO AO PROCESSO DE DISPENSA DE LICITAÇÃO

Integram o presente contrato, como se nele estivessem transcritas, as cláusulas e condições estabelecidas no processo de dispensa de Licitação que o originou, referido no preâmbulo deste instrumento, bem como a proposta da **CONTRATADA** apresentada no referido expediente, naquilo que não divirja deste ajuste.

CLÁUSULA DÉCIMA QUINTA – DA PUBLICIDADE

O **CONTRATANTE** será responsável pela publicação do resumo deste instrumento no Diário da Justiça Eletrônico (DJ-e) do Poder Judiciário do Estado da Bahia, no prazo de 10 (dez) dias corridos, contados a partir da sua assinatura.

CLÁUSULA DÉCIMA SEXTA – DO FORO

Fica eleito o Foro da Cidade do Salvador-Bahia, que prevalecerá sobre qualquer outro, por mais privilegiado que seja, para dirimir quaisquer dúvidas oriundas do presente Contrato.

CLÁUSULA DÉCIMA SÉTIMA – DAS DISPOSIÇÕES GERAIS

17.1 O **CONTRATANTE** não responderá por quaisquer compromissos assumidos perante terceiros pela **CONTRATADA**, ou seus prepostos, ainda que vinculados à execução do presente Contrato;

17.2 A inadimplência da **CONTRATADA**, com relação a quaisquer custos, despesas, tributos, exigências ou encargos previstos neste contrato, não transfere ao **CONTRATANTE** a responsabilidade pelo seu pagamento, nem poderá onerar o objeto do contrato.

17.3 Aplicar-se-á a Lei Estadual-BA nº 9.433/2005 para dirimir toda e qualquer questão legal relativa à execução deste contrato, em especial os casos omissos.

17.4 Fica assegurado ao **CONTRATANTE** o direito de alterar unilateralmente o Contrato, mediante justificação expressa, nas hipóteses previstas no inciso I do art. 143, para melhor adequação às finalidades de interesse público, desde que mantido o equilíbrio econômico-financeiro original do contrato e respeitados os demais direitos da **CONTRATADA**.

17.5 Não caracterizam novação eventuais variações do valor contratual resultantes de revisão de preços, de compensações financeiras decorrentes

das condições de pagamento nele previstas ou, ainda, de alterações de valor em razão da aplicação de penalidades.

17.6 Inexistindo disposição específica, as obrigações contratuais devem ser praticadas no prazo de 05 (cinco) dias.

E, por assim estarem justos e acordados, assinam o presente Contrato em 02 (duas) vias, de igual teor e forma, para que produza seus efeitos legais, após a publicação depois de lido e achado conforme.

Salvador, _____ de _____ de 2021.

Ministério Público do Estado da Bahia
Frederico Welington Silveira Soares
Superintendente de Gestão Administrativa

Stefanini Rafael Segurança e Defesa S.A.
Maria Magali Bredariol
Representante Legal

APENSO I
TERMO DE COMPROMISSO, SIGILO E CONFIDENCIALIDADE

Os abaixo-assinados, de um lado o **MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA**, CNPJ nº 04.142.491/0001-66, situado na cidade de Salvador, a 5ª Avenida, nº 750, Centro Administrativo da Bahia - CAB, doravante denominada **CONTRATANTE**, e de outro lado a **EMPRESA STEFANINI RAFAEL SEGURANÇA E DEFESA S.A.**, CNPJ nº 24.691.488/0001-09, estabelecida à Avenida Eusebio Matoso, nº 1375, Andar 8, Salas 801 e 802, Butantã, CEP 05423-905, São Paulo/SP, doravante denominada **CONTRATADA**, tem entre si justa e acertada, a celebração do presente **TERMO DE COMPROMISSO, SIGILO E CONFIDENCIALIDADE**, através do qual a **CONTRATADA** aceita não divulgar, salvo com autorização prévia e formal, segredos e informações sensíveis de propriedade do **CONTRATANTE,** e se compromete a praticar procedimentos de segurança da informação, em conformidade com as seguintes cláusulas e condições:

1. A **CONTRATADA** compromete-se a manter em caráter confidencial as informações abaixo mencionadas, mesmo após a eventual rescisão do contrato:

1.1 Política de segurança adotada pelo **CONTRATANTE** e configurações de hardware e software decorrentes;

1.2 Processo de instalação, configuração e customizações de produtos, ferramentas e equipamentos e atendimento aos itens de segurança, constantes do Edital de licitação;

1.3 Processo de implantação no ambiente do **CONTRATANTE**, de mecanismos de criptografia e autenticação utilizados;

1.4 Recomendações e implementações decorrentes do processo de consultoria;

1.5 Quaisquer dados que a **CONTRATADA** venha a ter conhecimento em decorrência da presente contratação, pertinentes a hardware, serviços e sistemas aplicativos do **CONTRATANTE**, cujo conhecimento por terceiros exponha o ambiente a riscos de invasão ou resulte na vulnerabilidade do mesmo.

1.6 Não fazer uso das informações prestadas pela **CONTRATANTE** que não seja em absoluto cumprimento ao contrato em questão.

2. A quebra da confidencialidade ou sigilo de informações obtidas na prestação de serviços ensejará multa, responsabilidade criminal na forma da lei, sem prejuízo de outras providências nas demais esferas. A **CONTRATADA** obriga-se a tomar as providências necessárias para assegurar que as informações confidenciais não sejam divulgadas por seus empregados ou agentes.

3. A **CONTRATADA** deve assegurar que todos os seus colaboradores envolvidos diretamente nas atividades objeto da presente contratação guardarão sigilo sobre as informações que porventura tiverem acesso, e que os mesmos se comprometerão a informar, imediatamente, ao seu superior hierárquico, qualquer violação das regras de sigilo, por parte dele ou de qualquer pessoa, inclusive nos casos de violação não intencional.

4. A **CONTRATADA** deverá seguir a Política de Segurança da Informação definida pelo **CONTRATANTE**.

5. O não cumprimento de quaisquer das cláusulas deste Termo implicará em responsabilização administrativa, civil e criminal, de acordo com a legislação vigente.

Em, _____ de _____ de 2021.

_____

Ministério Público do Estado da Bahia
Frederico Welington Silveira Soares
Superintendente
CONTRATANTE

_____

Stefanini Rafael Segurança e Defesa S.A.
Maria Magali Bredariol
Representante Legal
CONTRATADA

MINISTÉRIO PÚBLICO
DO ESTADO DA BAHIA

DESPACHO

Encaminhamos o presente expediente informando que não encontramos nenhuma necessidade de modificação e/ou ajustes no quanto apresentado no anexo ***proposta de minuta de contrato*** (0188921)

Documento assinado eletronicamente por **Iaçanã Lima de Jesus Carneiro** em 29/20/7271, às 1: 397, conforme art. 1º, III, "b", da Lei 11.410/7226.

A autenticidade do documento pode ser conferida no site https3/sei.sistemas.mpba.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=2 informando o código verificador **0189214** e o código CRC **924527B6**.

MINISTÉRIO PÚBLICO
DO ESTADO DA BAHIA

DESPACHO

Encaminhos o presente expediente à Assessoria Técnico-Jurídica para análise da contratação de serviços de realização de PENTEST por dispensa de licitação e respectiva minuta de contrato, já aprovada pela unidade interessada, constante no documento 0188921.

Solicitamos apoio deste setor consultivo, também, quanto à avaliação dos documentos de representação da Sra. Maria Magali Bredariol, em conjunto com a resposta da empresa a ser contratada no documento 0180214, após apontamento realizado por esta Coordenação no Item 3 do documento 0172752.

Documento assinado eletronicamente por **Mariana Nascimento Sotero Campos** em 29/20/7271, às 1: 3 . , conºorme artl 1", ltb, L4L, da 6ei 11lf 10/722. l

A autenticidade do documento pode ser conºerida no site https3/seilsistemasImp4aImpl4r/sei/controlador_externolphp?acao=documento_conºerir&id_orgao_acesso_externo=2 inºormando o código veriºicador **0189224** e o código CRC **EB60953D**l

MINISTÉRIO PÚBLICO
DO ESTADO DA BAHIA

DESPACHO

De ordem da Assessora de Gabinete, **encaminhe-se o presente procedimento à Diretoria de Tecnologia da Informação, para que atualize as propostas comerciais.**

Após, retorne-se.

Em 17 de setembro de 2021.

Bel. Gláucio Matos Santos de Cerqueira
Assistente de Gestão II
Apoio Processual ATJ/SGA
Matrícula 352.748

Documento assinado eletronicamente por **Glaucio Matos Santos Cerqueira** em 17/09/2021, às 17:09, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.sistemas.mpba.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0196592** e o código CRC **46CC2745**.

stefaninirafael

SERVIÇO
Teste de Intrusão e Rastreamento de Vulnerabilidades

CLIENTE
MPBA

MINISTÉRIO PÚBLICO
DO ESTADO DA BAHIA

Proposta Técnica Comercial n° 093708_20210713_2
24 de Setembro de 2021

Sumário

1. APRESENTAÇÃO 5

2. DADOS DA EMPRESA 6

3. INTRODUÇÃO 7

3.1 ESTRUTURAÇÃO DA PROPOSTA 7

4. SOBRE A STEFANINI RAFAEL 8

4.1 ALGUNS DOS CLIENTES DA STEFANINI RAFAEL 9
4.2 POSICIONAMENTO GLOBAL DA STEFANINI RAFAEL 9
4.3 SERVIÇOS OFERTADOS PELA STEFANINI RAFAEL 10

5. PROPOSTA TÉCNICA 11

5.1 ESCOPO 11
5.1.1 Conteúdo do Edital 11
5.1.2 Restrições ao Teste de Intrusão 12
5.1.3 Produtos de Entrega 13
5.1.4 Estimativa de Prazos 14
5.1.5 Recursos Necessários ao Projeto 14
5.2 METODOLOGIA DE GERÊNCIA DE PROJETO 16

6. RESPONSABILIDADES E PREMISSAS TÉCNICAS 17

6.1 EXCLUSÕES (UNDELIVERABLES) 17
6.2 PREMISSAS GERAIS 17
6.3 PREMISSAS DA CONTRATADA 17
6.4 PREMISSAS DO CONTRATANTE 18
6.5 RESPONSABILIDADES DO CONTRATANTE COM A CONTRATADA 18
6.6 RESPONSABILIDADES DA CONTRATADA COM O CONTRATANTE 18
6.7 DIREITOS DE PROPRIEDADE 19

7. PROPOSTA COMERCIAL 20

8. PREMISSAS COMERCIAIS 21

8.1 CONDIÇÕES DE PAGAMENTO 21
8.2 ÍNDICE DE REAJUSTE 21
8.3 DAS NOTIFICAÇÕES 21
8.4 REEQUILÍBRIO ECONÔMICO 21
8.5 RESCISÃO CONTRATUAL 22

9. TERMO DE ACEITE 23

ANEXO – MODELO DE RELATÓRIO 24

Anexo Orcamento 01_Atualizado.pdf (0202857) SEI 19.09.02684.0011790/2021-22 / pg. 647

Lista de Figuras

Figura 1 - Estrutura de Diretorias 8
Figura 2 - Clientes Stefanini Rafael 9
Figura 3 - Posicionamento global da Stefanini Rafael 9
Figura 4 - Fases PMBok 16
Figura 5 - Etapas de uma Sprint 16

Lista de Tabelas

Tabela 1 – Teste de Intrusão Aplicações Críticas 20

Anexo Orcamento 01_Atualizado.pdf (0202857) SEI 19.09.02684.0011790/2021-22 / pg. 648

Histórico

Data	Autor	Descrição	Versão
22/06/2021	Marco Alexandre Rodrigues	Criação do documento	1.00
13/07/2021	Alex Willian de Oliveira	Revisão da Proposta	2.00
24/09/2021	Claudio Lima	Revisão de Data	2.01

Responsável pela Proposta

E-mail: marco.rodrigues@stefaninirafael.com
Contato: +55 (11) 9 4192-3758

Validade da Proposta

Esta proposta tem validade de **60 dias**, a partir da data da emissão de sua última versão.

Data de emissão: 24/09/2021
Data de validade: 23/11/2021

Anexo Orcamento 01_Atualizado.pdf (0202857) SEI 19.09.02684.0011790/2021-22 / pg. 649

1. APRESENTAÇÃO

Ministério Público da Bahia

Prezados Senhores,

Segue o documento contendo as condições técnicas e comerciais para atendimento da solicitação cliente para o fornecimento de um serviço de teste de intrusão (*Pen Test*) e rastreamento de vulnerabilidades (*Vulnerability Scan*).

Este documento foi elaborado envolvendo as áreas de soluções, negócios e recursos humanos, que trabalhando em equipe criaram esta solução para atender ao requerido.

A Stefanini Rafael possui uma característica de forte adaptação ao cliente e o modelo de negócio apresentado nessa proposta é um primeiro balizador desenhado com premissas que podem ser alteradas caso haja esta necessidade.

Agradecemos o convite para participação nesta oportunidade e esperamos atender a todas as expectativas.

Estaremos à disposição para os esclarecimentos necessários.

Boa leitura.

Atenciosamente,

Leidivino Natal da Silva
CEO – Stefanini Rafael
natal.silva@stefaninirafael.com
+55 11 97130-5514

Anexo Orcamento 01_Atualizado.pdf (0202857) SEI 19.09.02684.0011790/2021-22 / pg. 650

2. DADOS DA EMPRESA

Dados oficiais

Razão Social: Stefanini Rafael Segurança e Defesa S.A.
Nome Fantasia: Stefanini Rafael Segurança e Defesa S.A.
CNPJ: 24.691.488/0001-09
Web Site: www.stefaninirafael.com.br

Matriz

Avenida Eusebio Matoso 1375, 8° Andar Sala 801 e 802
São Paulo UF: SP Cep: 05423-905

CEO

Leidivino Natal da Silva
CEO – Stefanini Rafael
natal.silva@stefaninirafael.com
+55 11 97130-5514

Representante Comercial

Patrícia Maia Dantas
Diretora de Negócios
pmdantas@stefanini.com
+55 71 9 9624-7432

Representantes Legais

Maria Magali Bredariol
Diretora Jurídica
mbredariol@latam.stefanini.com
+55 11 99934-2252

Luiz Carlos Marques de Aguiar
Diretor Financeiro
laguiar@stefanini.com
+55 11 97283-2530

3. INTRODUÇÃO

Para atender à solicitação cliente, desenvolvemos uma solução que está apresentada neste documento, que inclui o detalhamento técnico, entrega dos serviços e produtos, incluindo os métodos, ferramentas e equipe ofertada.

Nesta Proposta Técnica, demonstramos como entendemos o desafio apresentado pelo cliente e de como podemos atender a esta demanda, visando atender aos requisitos técnicos conforme solicitado durante reunião com a equipe técnica.

3.1 ESTRUTURAÇÃO DA PROPOSTA

A Proposta Técnica Comercial foi estruturada em documento único e contém o detalhamento do entendimento dos requisitos solicitados, entrega dos serviços e produtos, incluindo os métodos, ferramentas, equipes e infraestrutura ofertadas, além do valor do investimento, termos e condições comerciais.

Anexo Orcamento 01_Atualizado.pdf (0202857) SEI 19.09.02684.0011790/2021-22 / pg. 652

4. SOBRE A STEFANINI RAFAEL

A Stefanini Rafael Segurança e Defesa é uma **joint venture** entre a **Stefanini**, multinacional brasileira que atua no setor de serviços de tecnologia da informação, com a empresa **Rafael Advanced Defense Systems** de origem Israelense e conhecida mundialmente como uma das maiores empresas de soluções em Segurança & Defesa. A Stefanini Rafael Segurança e Defesa tem por objetivo atuar nas áreas de Segurança & Defesa no Brasil e América Latina, com soluções inovadoras e sistemas de alta tecnologia.

A Stefanini Rafael é composta no Brasil da Diretoria se Segurança Cibernética e Inteligência e da Diretoria de Comunicação.

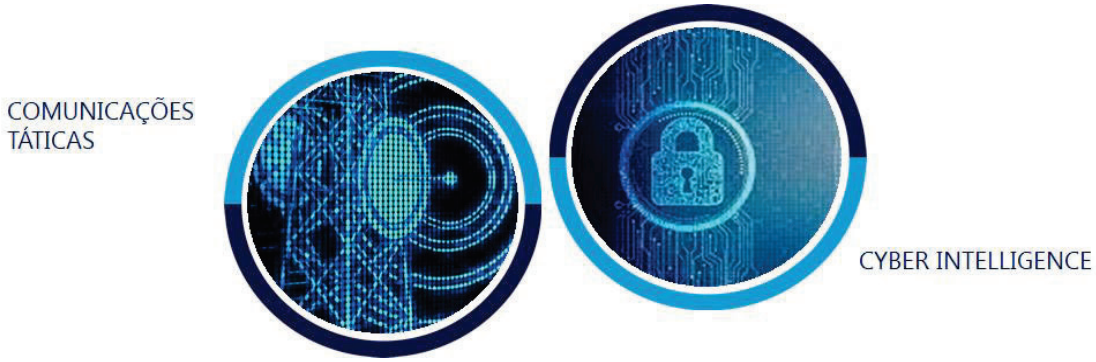


Figura 1 - Estrutura de Diretorias

MISSÃO	ESTRATÉGIA	VISÃO
Trabalhamos para concretizar os sonhos dos nossos clientes, colaboradores e acionistas, através da melhor tecnologia para soluções de Cyber, Segurança, Inteligência e Defesa.	Nossas decisões e nosso comportamento são movidos por valores importantes: agir com integridade, respeito, energia, atitude positiva e foco em resultados sustentáveis.	Com base em nossos valores, buscamos ser o melhor provedor de tecnologia, reconhecido como um parceiro estratégico, por agir com paixão e energia para conquistar e encantar os clientes.

Acesse nosso site e conheça mais em: http://www.stefaninirafael.com

4.1 Alguns dos clientes da Stefanini Rafael



Figura 2 - Clientes Stefanini Rafael

4.2 Posicionamento Global da Stefanini Rafael

A Stefanini Rafael tem como foco principal o mercado Brasileiro, porém já estamos posicionados em outros países e com planos de expansão para outros mercados:

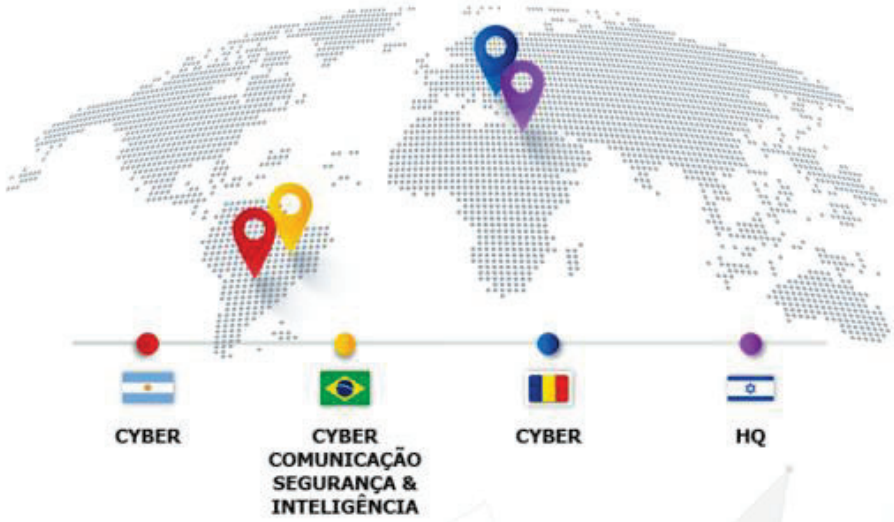


Figura 3 - Posicionamento global da Stefanini Rafael

Anexo Orcamento 01_Atualizado.pdf (0202857) SEI 19.09.02684.0011790/2021-22 / pg. 654

4.3 Serviços ofertados pela Stefanini Rafael

Plano Estratégico	• Desenvolvimento de políticas de segurança da informação; • Gestão de riscos e conformidades; • Auditoria Independente de Segurança da Informação;
Plano Tático	• Consultoria de Segurança da Informação – Governança; • Suporte para certificações como PCI-DSS, ISO 27000/05; • Auditoria Independente de Segurança da Informação; • Venda de produtos e serviços dos maiores players de mercado;
Plano Operacional	• Pentest (Black-Box, White Box e Gray Box); • Teste de vulnerabilidades de softwares e códigos; • Monitoramento de respostas a incidentes de segurança; • Gestão de segurança da informação de empresas clientes; • Alocação de profissionais de segurança no ambiente de T.I. do cliente. (body shop); • Monitoramento e avaliação de riscos de segurança na Deep e na Dark Web; • Treinamentos para clientes.

Anexo Orcamento 01_Atualizado.pdf (0202857) SEI 19.09.02684.0011790/2021-22 / pg. 655

5. PROPOSTA TÉCNICA

Esta proposta técnica visa atender aos requisitos solicitados pelo cliente **Ministério Público da Bahia** para a prestação de serviços técnicos de segurança cibernética. O escopo deve atender ao documento “Especificação Técnica MP BA - Pentest Voto Eletrônico” publicado pelo Contratante.

5.1 Escopo

O escopo técnico desta proposta refere-se à prestação de serviço de teste de intrusão (*Pentest*).

Características deste projeto:

- Teste de Intrusão tipo **Black Box** de **1 aplicações críticas (1x URL)**.
- O serviço será prestado de **forma remota.**
- O cliente deverá preencher **autorização prévia para a realização dos serviços**.

Os produtos finais desta proposta:

- Teste de Intrusão:
  - Identificar modos de explorar as vulnerabilidades a fim de enganar ou anular os recursos de segurança dos componentes do sistema.
  - Cliente deverá identificar os endereços das dez aplicações críticas.

5.1.1 Conteúdo do Edital

Reprodução de conteúdo do documento “Especificação Técnica MP BA - Pentest Voto Eletrônico” publicado pelo Contratante.

A atividade de Teste de Intrusão/Penetração (Pentest) deve compreender o teste de Invasão externa e tem como objetivo principal identificar, possíveis vulnerabilidades na **aplicação WEB** VOTO ELETRÔNICO da CONTRATANTE. Estes testes envolvem o uso de técnicas e ferramentas para tentar o acesso privilegiado aos ativos e informações da CONTRATANTE por meio de simulações controladas de ataques reais, sendo o ambiente da aplicação da CONTRATANTE avaliado em sua totalidade em busca de vulnerabilidades que possam permitir a obtenção de acesso não-autorizado, sendo que a modalidade de teste de intrusão/penetração a ser realizado será do tipo **Black Box**.

O teste Black Box parte da premissa que o profissional não tem informações sobre o sistema nem da estrutura da empresa e trata a aplicação como uma “caixa preta”. Sendo mais difícil de ser aplicado, já que é preciso colher algumas informações para tentar explorar vulnerabilidades, mas em compensação, essa simulação fica mais próxima de um ataque real feito externamente por um hacker.

A CONTRATADA deverá realizar **1 teste intrusão** para identificação de vulnerabilidades por meio de simulações de invasão de serviços e infraestrutura (Teste de Invasão) a serem executadas externamente (através da Internet), com duração de **até 20 (vinte) dias**.

A CONTRATADA deverá elaborar “Relatório de Teste de Invasão” para cada teste realizado apresentando todas as informações sobre o mesmo, contemplando no mínimo: objetivos, premissas e escopo do teste; metodologia de análise de

vulnerabilidades; descrição das ações realizadas; vulnerabilidades encontradas; categorização e severidade das vulnerabilidades, recomendações e controles de segurança necessários para correção das vulnerabilidades; apresentação das evidências; referências e ferramentas utilizadas.

A Metodologia adotada pela CONTRATADA durante o Pentest deve incluir minimamente, quando pertinente, as seguintes vulnerabilidades:

1. Injeção de Código.
2. Quebra de Autenticação.
3. Exposição de Dados Sensíveis.
4. Entidades Externas de XML.
5. Quebra de Controle de Acesso.
6. Configuração Incorreta de Segurança.
7. Cross-Site Scripting (XSS).
8. Desserialização Insegura.
9. Utilização de Componentes com Vulnerabilidades Conhecidas.
10. Log e Monitoramento Ineficientes.

A CONTRATADA deverá minimamente compreender atividades que busquem encontrar vulnerabilidades em potencial, de eventual má configuração, de falhas em hardwares e softwares desconhecidos, de técnicas de contramedidas ou deficiências na infraestrutura ou sistemas da CONTRATANTE.

A CONTRATANTE deve criar **um usuário interno para a CONTRATADA** no ambiente da CONTRATANTE com todas suas ações logadas para documentação e atestar a integridade do trabalho realizado pela CONTRATADA.

O alvo do PENTEST (Teste de Invasão) será a aplicação aqui denominada VOTO ELETRÔNICO. Todas as fases dos PENTEST poderão ser acompanhadas e supervisionadas a qualquer momento pelo CONTRATANTE. Quaisquer atividades com suspeita de comprometimento de algum ambiente ou ativo, deverá a CONTRATADA ser reportada pelo CONTRATANTE.

Os serviços contratados deverão ser obrigatoriamente executados fora das dependências da CONTRATANTE.

O teste de penetração incluirá as seguintes técnicas de teste:

- Ping sweep de intervalos de redes;
- Verificação de portas de hosts de destino;
- Verificação de vulnerabilidades dos alvos;
- Penetração em alvos;
- Manipulação no nível do aplicativo;
- Engenharia reversa Java / ActiveX do lado do cliente;
- Ataques de negação de serviço;
- Verificações / explorações perigosas.

5.1.2 Restrições ao Teste de Intrusão

Os métodos, técnicas e ferramentas deverão ser selecionadas pelo *Ethical Hacker*, conforme o escopo, o tipo de aplicação e as restrições impostas pelo cliente. Não há a

obrigatoriedade de utilizar todos os métodos, técnicas e ferramentas para todos os projetos.

Os métodos, técnicas e ferramentas apresentados, podem afetar a performance e até mesmo interromper o uso de alguns equipamentos momentaneamente. Desta forma, a escolha dos métodos e técnicas deverão ser avaliados conforme cada cliente, infraestrutura, severidade dos testes e importância dos equipamentos.

Métodos que aplicam dicionário de senhas e *brute force* tendem a ser mais agressivos ao ponto de afetar os equipamentos servidores. Não há nestes casos, como garantir que o teste não afetara o servidor/sistema.

No entanto vale ressaltar que estes testes apresentam respostas muito positivas no contexto da análise de intrusão e são métodos comuns e muito usados por Black Hackers. Assim o teste de intrusão com estes testes serve também para mostrar a resiliência do servidor/sistema ante a ataques similares no mundo real.

Uma opção para mitigar este problema é agendar os testes nos horários com menor uso e tráfego de dados pelos servidores, evitando a queda de performance ou indisponibilidade.

Outro ponto importante é que toda ação da equipe Stefanini Rafael, só será realizada após autorização formal do cliente, com o consentimento de execução, os riscos conhecidos, o tipo de teste e os horários programados de execução.

5.1.3 Produtos de Entrega

Os produtos de entrega previstos (*Deliverables*), consistem em um relatório que deverá reportar as estratégias e métodos utilizados para realizar a análise de segurança e os resultados de vulnerabilidades encontradas, assim como sugestões pra a equipe técnica do cliente.

O relatório do Teste de Intrusão deve conter a descrição de cada problema verificado e/ou possível problema descoberto. Riscos mais específicos que a vulnerabilidade pode representar, incluindo métodos específicos como e até que ponto ele pode ser explorado (Eliminação, mitigação, aceitação). Exemplos de vulnerabilidades incluem, entre outros, injeção de SQL, escalonamento de privilégio, script entre sites ou protocolos obsoletos.

O relatório do Rastreamento de Vulnerabilidades deve evidenciar os riscos potenciais apresentados por vulnerabilidades conhecidas, classificados de acordo com as pontuações associadas a cada vulnerabilidade.

Os relatórios finais têm por objetivo:

- Relatar os resultados obtidos.
- Dar suporte à equipe de segurança e de operação para solucionar os principais problemas de segurança no ambiente.
- Servir como métrica para medir à maturidade do negócio da empresa e a sua importância com a segurança, além de medir o trabalho da equipe de segurança sobre a aplicação das melhores práticas de proteção.
- Servir como uma prova dos testes realizados e de que tudo foi devidamente realizado sem fugir do escopo determinado.

Anexo Orcamento 01_Atualizado.pdf (0202857) SEI 19.09.02684.0011790/2021-22 / pg. 658

- Prover informações relevantes sobre os testes realizados no ambiente caso haja um incidente durante ou posteriormente, após os testes de vulnerabilidade.

5.1.4 Estimativa de Prazos

As entregas referentes a esta proposta devem seguir aos prazos aqui estimados para a análise em um web site (URL), uma API ou um Aplicativo Móvel:

Método Black Box

- 40 a 80 horas de execução
- Realização estimada em 10 - 20 dias úteis consecutivos

5.1.5 Recursos Necessários ao Projeto

Detalha-se a seguir a infraestrutura necessária para este projeto.

5.1.5.1 Acessos

Para melhor entregar e testar as vulnerabilidades existentes no ambiente do cliente será necessário um usuário com poder administrativo na árvore de domínio. Dessa maneira será possível acessar vulnerabilidades que são encontradas dentro de sistemas operacionais dos dispositivos existentes no ambiente de rede. Esta exigência está atrelada a análise de rede interna e depende do método de análise escolhido.

5.1.5.2 Infraestrutura

O cliente deve prover à Stefanini Rafael, caso necessário, um ambiente de trabalho para a equipe técnica que necessitar trabalhar alocada na estrutura física do cliente, como mesas, cadeiras, entradas de energia e conexões à rede tantas quanto forem necessárias.

Este ambiente deve ser restrito e em local afastado dos demais colaboradores para evitar que as informações coletadas durante o processo de análise de vulnerabilidades percam a confidencialidade, pois podem trazer informações sensíveis ao ambiente e causar dados irreparáveis tanto ao ambiente quanto à integridade do cliente.

5.1.5.3 Autorizações

O cliente deve prover à Stefanini Rafael, caso necessário, autorização formal para acesso ao ambiente digital onde serão realizadas as análises.

5.1.5.4 Questionário Inicial

O cliente deve prover à Stefanini Rafael, o documento intitulado “Questionário de Pen Test”, para que nossos especialistas possam preparar melhor a estratégia de análise a ser aplicada.

Exemplos de algumas questões relativas ao processo de análise:

- Quais hosts específicos, intervalos de endereços de rede ou aplicativos devem ser testados?
- Quais hosts específicos, intervalos de endereços de rede ou aplicativos não devem ser explicitamente testados?
- O teste será realizado em um ambiente de produção ao vivo ou em um ambiente de teste?
- Os ataques de negação de serviço são permitidos?

Anexo Orcamento 01_Atualizado.pdf (0202857) SEI 19.09.02684.0011790/2021-22 / pg. 659

- As verificações e explorações perigosas são permitidas?

Anexo Orcamento 01_Atualizado.pdf (0202857) SEI 19.09.02684.0011790/2021-22 / pg. 660

5.2 Metodologia de Gerência de Projeto

Todos os projetos da Stefanini Rafael utilizam os preceitos do Guia PMBOK (*Project Management Body of Knowledge*), que consiste em uma publicação do *Project Management Institute*, PMI, que compila as melhores práticas mundialmente aceitas em Gerenciamento de Projetos.

O Guia PMBOK identifica um subconjunto de conhecimentos em gerenciamento de projetos, que é amplamente reconhecido como boas práticas. Uma boa prática não significa que o conhecimento e as práticas devem ser aplicados uniformemente a todos os projetos, sem considerar se são ou não apropriados.

O Guia PMBOK também fornece e promove um vocabulário comum para se discutir, escrever e aplicar o gerenciamento de projetos possibilitando o intercâmbio eficiente de informações entre os profissionais de gerência de projetos.

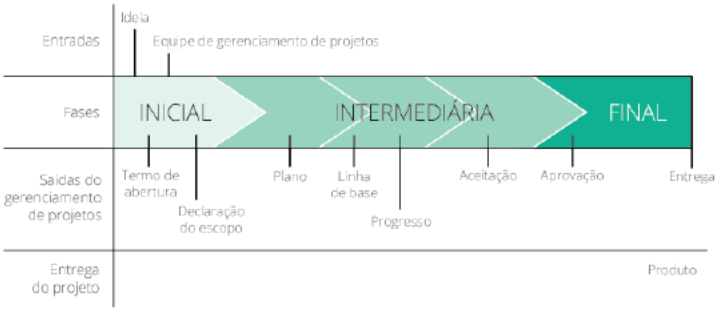


Figura 4 - Fases PMBok

Para projetos que envolvem o desenvolvimento de sistemas ou alocação de *squads* no cliente, a gestão de projetos pode ainda associar o *Framework Scrum* para a gestão com o Conceito Ágil.



Figura 5 - Etapas de uma Sprint

Anexo Orcamento 01_Atualizado.pdf (0202857) SEI 19.09.02684.0011790/2021-22 / pg. 661

6. RESPONSABILIDADES E PREMISSAS TÉCNICAS

Para este capítulo devemos considerar a nomenclatura:

- Contratante: Cliente ou empresa contratante do serviço.
- Contratada: Prestador do serviço contratado.
- Partes: Ambas as empresas. Responsabilidade de ambas as partes.

6.1 Exclusões (Undeliverables)

- Este serviço não prevê análises Antispam ou de Phishing em repositórios ou domínios de e-mail.
- Este serviço não prevê a execução de atividades de correção ou de mitigação de riscos, sendo o objeto desta proposta apenas a avaliação das informações, testes, análise documental e entrega dos relatórios finais para o cliente com as proposições de melhorias.

6.2 Premissas Gerais

- Todas as atividades apresentadas nesta proposta consideram a efetiva participação do Contratante.
- É de responsabilidade das Partes a não divulgação de dados ou informações relacionadas aos produtos objetos do presente, mantendo sigilo absoluto em relação a todos os dados acessados ou que venham a ser gerados no processo de prestação dos serviços. Desta forma, todos os documentos relativos a este projeto, incluindo esta proposta, estão classificados como documento confidencial.
- As datas, horários e cronograma para a execução das atividades aqui propostas serão devidamente acordados entre as Partes, após a assinatura do contrato.
- As estimativas de tempo e custo desta proposta foram criadas com base nas informações fornecidas pelo Contratante durante a elaboração deste documento, de forma que o escopo a ser executado é o descrito neste documento.
- Caso haja a necessidade de executar atividades fora dos horários comerciais ou em finais de semana ou feriados, deverá ocorrer acréscimos nos valores da mão de obra, conforme previsto na legislação trabalhista atual.
- Caso haja necessidade de incorrer em custos adicionais, a Contratada só o fará com a anuência do Contratante.

6.3 Premissas da Contratada

- A execução das atividades previstas nesta proposta já confere automaticamente a autorização para o pagamento.
- O gerente de projetos e/ou gerente de delivery da Contratada terá independência para gerenciar toda a sua equipe.
- As horas improdutivas são caracterizadas pelas situações onde os consultores da Contratada estão disponíveis para realizar as suas atividades, mas os trabalhos não podem evoluir por conta de um eventual descumprimento de cronograma por parte do Contratante, como: falta no fornecimento de informações, pré-requisitos e premissas não atendidos, indisponibilidade de

Anexo Orcamento 01_Atualizado.pdf (0202857) SEI 19.09.02684.0011790/2021-22 / pg. 662

equipamentos, indisponibilidade de pessoal do cliente, indisponibilidade de outros fornecedores do cliente que estejam envolvidos nas atividades de projeto, dentre outros aspectos similares. Horas improdutivas contam como tempo de projeto para o cálculo dos honorários em favor da Contratada.

- Integrantes do time Contratante não poderão ser contratados ou terceirizados pela Contratante, seja dentro do período de prestação dos serviços, ou em até 3 (três) meses após a entrega dos serviços contratados, sob pena de indenização correspondente à média dos últimos 3 (três) meses de serviços prestados.

6.4 Premissas do Contratante

- Integrantes do time Contratada não poderão ser contratados ou terceirizados pela Contratante, seja dentro do período de prestação dos serviços, ou em até 3 (três) meses após a entrega dos serviços contratados, sob pena de indenização correspondente à média dos últimos 3 (três) meses de serviços prestados.

6.5 Responsabilidades do Contratante com a Contratada

- Designar um colaborador principal (Preposto) que será o ponto focal com o time da Contratada. Este preposto deverá ter poder de decisão e acessos executivos que vierem a ser necessários. Responsabilidades:
  - Acompanhamento dos serviços,
  - Agendamento de interações com equipes internas,
  - Resolução de situações que possam gerar atrasos ou problemas ao projeto,
  - Designar novo preposto em situações de férias ou ausências temporárias.
- Fornecer todas as informações necessárias e pertinentes ao assunto, em tempo hábil, sem qualquer forma de reserva ou censura.
- Disponibilizar a infraestrutura necessária (sala de reunião, mesas, cadeiras) para o desenvolvimento dos trabalhos, de acordo com a necessidade.
- Disponibilizar pessoas responsáveis pelos processos, as quais possam apoiar nossos engenheiros a entender a topologia de rede ou aplicações do cliente.
- Disponibilidade de equipe local de apoio durante as visitas de nossa equipe no local.
- Fornecer às nossas equipes usuários e permissões de acesso conforme necessário.
- Fornecer às nossas equipes arquitetura e topologia de rede do sistema, lista de fornecedores de soluções de terceiros e mecanismos de integração conforme necessário.
- Fornecer todas as informações necessárias e pertinentes ao assunto, em tempo hábil, sem qualquer forma de reserva ou censura.
- Disponibilizar a infraestrutura necessária (sala de reunião, mesas, cadeiras) para o desenvolvimento dos trabalhos, de acordo com a necessidade.

6.6 Responsabilidades da Contratada com o Contratante

- Contratar profissionais qualificados, compatíveis com a complexidade e atribuições dos serviços apresentados nessa proposta.
- Assegurar a boa conduta dos profissionais, considerando sempre as políticas internas do cliente.

6.7 Direitos de propriedade

Todos os relatórios ou documentos gerados durante esse serviço serão de propriedade exclusiva do Contratante.

Anexo Orcamento 01_Atualizado.pdf (0202857) SEI 19.09.02684.0011790/2021-22 / pg. 664

7. 0.312PROPOSTA COMERCIAL

Os valores apresentados nas tabelas abaixo referem-se aos métodos aplicáveis de Testes de Intrusão, cada qual com suas características técnicas e particularidades.

Prestação de Serviços Técnicos Teste de Intrusão (Pentest) Aplicação Web	**Preço Total**
Método Black Box (40 horas de execução)	R$ 8.202,67
Análise de um endereço Web (URL)	
Incluso análise em até três APIs por endereço Web	

Tabela 1 – Teste de Intrusão Aplicações Críticas

Para aplicações críticas (Web), os valores apresentados na tabela 1, se referem a uma única Aplicação Web (URL), com a análise de no máximo três APIs.

As opções apresentadas na Tabela 1 representam a aplicação do Teste de Intrusão uma única vez, para uma aplicação crítica.

Caso haja necessidade de testes mais complexos, com um número maior de APIs, existe a possibilidade de um ajuste nos valores apresentados nesta tabela, o qual será objeto de nova proposta.

Faz-se mister ressaltar que estas análises podem também concluir que o cliente não possui vulnerabilidades na aplicação analisada. Este é um risco que pode ocorrer neste processo, e que neste caso, mostraria que a aplicação do cliente está atualizada e aderente aos melhores padrões de segurança do mercado.

Anexo Orcamento 01_Atualizado.pdf (0202857) SEI 19.09.02684.0011790/2021-22 / pg. 665

8. PREMISSAS COMERCIAIS

8.1 Condições de Pagamento

Seguem condições:

- As notas fiscais deverão ser emitidas no 1º dia útil de cada mês subsequente à prestação do serviço.
- Prazo de vencimento será de até 15 dias da data de sua emissão.
- Todos os impostos estão inclusos no preço apresentado (ISS, IR, PIS, COFINS, CSSL).
- O pagamento será realizado através depósito bancário (transferência, DOC ou TED).
- Qualquer quantia que não seja paga na data do vencimento combinado será acrescida de correção monetária, calculada de acordo com a variação do IPCA-IBGE, e juros de mora de 1% (um por cento) ao mês, tudo corrigido, *pro-rata temporis*, além do pagamento de multa moratória no importe de 2% (dois por cento) dos valores em atraso, que serão imediatamente devidos e pagáveis à Stefanini Rafael.

8.2 Índice de Reajuste

Os preços dos serviços serão reajustados anualmente, a partir da assinatura do contrato/aditivo, na variação positiva do IGPM anual e/ou índice de mercado.

8.3 Das Notificações

Eventuais retenções, deduções ou compensações previstas no presente instrumento contratual, somente serão válidas e se concretizarão quando da prévia notificação por escrito, com antecedência mínima de 15 (quinze) dias corridos à Contratada, explicitando detalhadamente os motivos pelos quais tais ações serão praticadas.

As retenções, deduções ou compensações somente ocorrerão após a possibilidade de defesa da Contratada, garantindo-se o direito à ampla defesa e ao contraditório dentro de prazo razoável. Qualquer retenção arbitrária por parte da Contratante ensejará na devolução imediata do valor retido à Contratada, bem com multa de 15% sobre o valor retido, sem prejuízos das perdas e danos.

8.4 Reequilíbrio Econômico

Em caso de alterações de ordem econômica advindas de medidas governamentais futuras ou quanto a legislação tributária e/ou previdenciária em vigor nesta data, de modo a modificar, majorar ou reduzir os tributos e encargos incidentes sobre as operações aqui pactuadas, assim como pela instituição ou extinção de outros impostos, taxas, contribuições especiais de qualquer natureza, restituíveis ou não, que venham a incidir ou repercutir sobre este ajuste e/ou seu objeto, a Stefanini Rafael atualizará os valores contratuais e informará à Contratante, de forma a manter o equilíbrio econômico-financeiro do contrato, conforme disposto nos artigos 478 e 479 do código civil brasileiro.

8.5 Rescisão Contratual

Poderá o contrato ser cancelado por instrumento consensual firmado entre as Partes, nas condições pactuadas pelas mesmas na ocasião do cancelamento.

As Partes poderão rescindir o presente contrato, independentemente de qualquer notificação judicial ou extrajudicial, nas seguintes hipóteses:

I. Inadimplência reiterada de qualquer cláusula ou condição do presente contrato, não sanada no prazo estabelecido em notificações prévias.
II. Decretação de falência, insolvência ou recuperação judicial da Contratada ou da Contratante.
III. Nos demais casos previstos na legislação em vigor.
IV. Atraso nos pagamentos combinados, superiores a 30 (trinta) dias, contados dos respectivos vencimentos, pela Contratante.

9. TERMO DE ACEITE

Data da Proposta
setembro 24, 2021

Nome

Cargo

Assinatura Data / /

☐ Aceito os termos

Aplicação Críticas - Descrever a URLs / IPs:

Aplicação de voto eletrônico

URL:

Range de IPs:

Tipo de Teste:

☐ White Box ☐ Grey Box ☒ Black Box

Anexo Orcamento 01_Atualizado.pdf (0202857) SEI 19.09.02684.0011790/2021-22 / pg. 668

ANEXO – MODELO DE RELATÓRIO



Relatório de Pentest – Target a ser testado

Versão: 1.00 Sigiloso - Restrito

stefaninirafael

Documento	Emitido em	Responsável
Relatório de Pentest – Target a ser testado	DD-Mês-AAAA	Nome do responsável pelo teste
Cliente	**Projeto**	
Empresa X	Pentest – target a ser testado	

Sumário

1. OBJETIVO 4

2. INTRODUÇÃO 5

3. ESCOPO DO PENTEST 6

3.1 EXCLUSÕES DO ESCOPO DE PENTEST 7

4. VULNERABILIDADES DOS ATIVOS 8

5. VULNERABILIDADES EXPLORADAS 9

5.1 VULNERABILIDADES WEB E DE INFRAESTRUTURA 9

5.1.1 Vulnerabilidades de Risco Alto 9

5.1.1.1 Dispositivos com SSLv3 e/ou TLSv1.0 habilitados 9

5.1.2 Vulnerabilidades de Nível Médio 9

5.1.2.1 Equipamentos com CVEs relacionados a patches de atualização pendentes: 9

5.1.2.2 Arquivos Javascript e JSON expostos na aplicação: 10

5.1.2.3 Enumeração da versão do OpenSSH disponível 10

5.1.3 Vulnerabilidades de Nível Baixo 11

5.1.3.1 URLs com falta de header de prevenção à X-Frame: 11

5.1.3.2 Cookie não tem flag HttpOnly 11

5.1.3.3 Cookie não tem flag Secure 11

5.1.3.4 Cookie de sessão sem expiração 12

5.2 VULNERABILIDADES DO APLICATIVO 12

5.2.1 Vulnerabilidades de Risco Alto 12

5.2.1.1 Aplicativo com mais permissionamentos que o necessário: 12

5.2.1.2 Aplicativo sem restrições de configurações: 12

ANEXO A – PENTEST DD DE MÊS DE AAAA 13

QUESTIONÁRIO DE ESCOPO DE PENTEST: 13

EVIDÊNCIAS DAS VULNERABILIDADES EXPLORADAS: 13

Anexo Orcamento 01_Atualizado.pdf (0202857) SEI 19.09.02684.0011790/2021-22 / pg. 670

stefaninirafael

Documento	Emitido em	Responsável
Relatório de Pentest – Target a ser testado	DD-Mês-AAAA	Nome do responsável pelo teste
Cliente	**Projeto**	
Empresa X	Pentest – target a ser testado	

Histórico

Data	Autor	Aprovador	Descrição	Versão
Dd/mm/aaaa	Nome do autor	N/A	Criação do documento	1.00

Anexo Orcamento 01_Atualizado.pdf (0202857) SEI 19.09.02684.0011790/2021-22 / pg. 671

stefaninirafael

Documento	Emitido em	Responsável
Relatório de Pentest – Target a ser testado	DD-Mês-AAAA	Nome do responsável pelo teste
Cliente	**Projeto**	
Empresa X	Pentest – target a ser testado	

1. OBJETIVO

O objetivo deste documento é apresentar o resultado técnico da avaliação da execução de Pentest e Scan de Vulnerabilidades executado nas URLs e APIs que compõe o aplicativo da Empresa X.

Este documento apresentará o escopo da execução de Pentest e Scan de Vulnerabilidades de acordo com o Questionário de Escopo de Pentest respondido pelo responsável técnico da Empresa X, além disso, será apresentado o resultado da análise e evidências de vulnerabilidades encontradas na infraestrutura, website e Aplicativo da Empresa X.

Anexo Orcamento 01_Atualizado.pdf (0202857) SEI 19.09.02684.0011790/2021-22 / pg. 672

stefaninirafael

Documento	Emitido em	Responsável
Relatório de Pentest – Target a ser testado	DD-Mês-AAAA	Nome do responsável pelo teste
Cliente	**Projeto**	
Empresa X	Pentest – target a ser testado	

2. INTRODUÇÃO

A Empresa X, com o intuito identificar e mapear vulnerabilidades em seu website/rede/aplicativo móvel, firmou através de um contrato uma parceria com à Stefanini Rafael, que tem como objetivo analisar, identificar e mapear vulnerabilidades no aplicativo da Empresa X, utilizando de técnicas de testes de invasão (Pentest). Para esta parceria, contemplado no escopo deste projeto, a Empresa X visa compreender se seu aplicativo apresenta fragilidades e possibilidades de estarem expostos a ataques cibernéticos.

Este relatório irá apresentar o resultado de análise de pentest e de scan de vulnerabilidades.

Anexo Orcamento 01_Atualizado.pdf (0202857) SEI 19.09.02684.0011790/2021-22 / pg. 673

stefaninirafael

Documento	Emitido em	Responsável
Relatório de Pentest – Target a ser testado	DD-Mês-AAAA	Nome do responsável pelo teste
Cliente	**Projeto**	
Empresa X	Pentest – target a ser testado	

3. ESCOPO DO PENTEST

Para definição do tipo de Pentest e o escopo de atuação utilizamos as respostas do Questionário de escopo de Pentest, disponível na seção de Anexo I deste documento. Após análise do questionário respondido, solicitamos recursos para acesso ao ambiente e iniciamos o trabalho.

O trabalho inicial do Pentest é identificar a quantidade de ativos, mapear os ativos críticos ou que não necessitam de avaliação.

Após o mapeamento dos ativos da rede informada ou da unidade de negócio, definimos que o escopo de trabalho do Pentest será avaliar os ativos mapeados.

Desta forma, na Tabelas abaixo, apresentamos todos os ativos mapeados que serão escopo do Pentest.

Aplicativos
Aplicativo 1.apk/.ipa

Tabela 1 - Aplicativos

URL	IP
Urlteste.com.br	100.0.0.1

Tabela 2 - Mapeamento de URLs

Ativos de rede	IP
Ativo 1	10.0.0.1
Ativo 2	10.0.0.2
Ativo 3	10.0.0.3

Tabela 3 - Mapeamento de ativos de rede

Anexo Orcamento 01_Atualizado.pdf (0202857) SEI 19.09.02684.0011790/2021-22 / pg. 674

stefaninirafael

Documento	Emitido em	Responsável
Relatório de Pentest – Target a ser testado	DD-Mês-AAAA	Nome do responsável pelo teste
Cliente	**Projeto**	
Empresa X	Pentest – target a ser testado	

3.1 Exclusões do escopo de pentest

Ativos de rede	IP
Ativo 1	10.0.0.1
Ativo 2	10.0.0.2
Ativo 3	10.0.0.3

Tabela 4 - Ativos Excluídos do teste

Anexo Orcamento 01_Atualizado.pdf (0202857) SEI 19.09.02684.0011790/2021-22 / pg. 675

stefaninirafael

Documento	Emitido em	Responsável
Relatório de Pentest – Target a ser testado	DD-Mês-AAAA	Nome do responsável pelo teste
Cliente	**Projeto**	
Empresa X	Pentest – target a ser testado	

4. VULNERABILIDADES DOS ATIVOS

Após mapeados todos os recursos do aplicativo da Empresa X, iniciamos o trabalho para identificar vulnerabilidades neles.

Executamos ferramentas e scripts e verificamos que existem vulnerabilidades no aplicativo da Empresa X às quais precisam ser tratadas a fim de prevenir possíveis invasões e/ou roubos de informações. As vulnerabilidades encontradas serão descritas nas sessões subsequentes deste relatório com base em sua criticidade em relação ao vazamento de informações.

Quantidade Total	Quantidade	Nível de Risco	Vulnerabilidade
12	1	Médio	Dispositivos com falta de aplicação de patches de atualização e segurança
	11	Médio	Arquivos Javascript e JSON expostos no website
2	1	Baixo	Servidor web sem Flags de segurança setadas
	1	Baixo	Cookie de sessão sem tempo de expiração

Tabela 5 - Vulnerabilidades web e de Infraestrutura

Quantidade Total	Quantidade	Nível de Risco	Vulnerabilidade
6	4	Alto	Aplicativo com mais permissionamentos que o necessário
	2	Alto	Aplicativo sem restrições de configurações

Tabela 6 - Vulnerabilidades do aplicativo

Anexo Orcamento 01_Atualizado.pdf (0202857) SEI 19.09.02684.0011790/2021-22 / pg. 676

stefaninirafael

Documento	Emitido em	Responsável
Relatório de Pentest – Target a ser testado	DD-Mês-AAAA	Nome do responsável pelo teste
Cliente	**Projeto**	
Empresa X	Pentest – target a ser testado	

5. VULNERABILIDADES EXPLORADAS

5.1 Vulnerabilidades web e de Infraestrutura

5.1.1 Vulnerabilidades de Risco Alto

5.1.1.1 Dispositivos com SSLv3 e/ou TLSv1.0 habilitados

Foram encontrados diversos equipamentos com SSLv3 e/ou TLSv1.0 habilitados.
Por se tratar de protocolos já extintos, esta vulnerabilidade permite a quebra de criptografia do tráfego de informações nos dispositivos em questão, consequentemente, as informações uma vez em texto limpo, podem ser capturadas e vazadas na rede mundial de computadores (internet).
As evidências relacionadas a esta vulnerabilidade estão presentes no Anexo I na última sessão deste relatório.

Solução: Habilitar as versões do TLSv1.1 ou superior nos dispositivos e desabilitar o SSLv3 e TLSv1.0 dos mesmos.
.

5.1.2 Vulnerabilidades de Nível Médio

5.1.2.1 Equipamentos com CVEs relacionados a patches de atualização pendentes:

Foram identificados CVEs provenientes da falta de aplicação de atualizações nos equipamentos que hospedam a aplicação. A falta destes patches pode expor informações internas no equipamento em questão
As evidências relacionadas a esta vulnerabilidade estão presentes no Anexo I na última sessão deste relatório.

Solução: Aplicar os paches de atualização e segurança pendentes nos equipamrentos.

Anexo Orcamento 01_Atualizado.pdf (0202857) SEI 19.09.02684.0011790/2021-22 / pg. 677

stefaninirafael

Documento	Emitido em	Responsável
Relatório de Pentest – Target a ser testado	DD-Mês-AAAA	Nome do responsável pelo teste
Cliente	**Projeto**	
Empresa X	Pentest – target a ser testado	

5.1.2.2 Arquivos Javascript e JSON expostos na aplicação:

Foram identificados arquivos Javascript e JSON expontos na aplicação que poder ser manipulados e utilizados para obter informações do sistema e/ou aplicativo.
As evidências relacionadas a esta vulnerabilidade estão presentes no Anexo I na última sessão deste relatório.

Solução: Adicionar os caminhos/extensões no arquivo robots.txt para que estes arquivos não fiquem mais visíveis.

5.1.2.3 Enumeração da versão do OpenSSH disponível

Foi possível enumerar a versão do SSH em alguns equipamentos. Com esta informação é possível explorar ataques de autenticação anônima e brute forcing nos mesmos, a fim de conseguir acesso ao equipamento e, posteriormente, realizar a coleta de informações sensíveis do ambiente.
As evidências relacionadas a esta vulnerabilidade estão presentes no Anexo I na última sessão deste relatório.

Solução: Desabilitar o banner com a versão do SSH e filtrar a conexão apenas para hosts internos.

Anexo Orcamento 01_Atualizado.pdf (0202857) SEI 19.09.02684.0011790/2021-22 / pg. 678

stefaninirafael

Documento	Emitido em	Responsável
Relatório de Pentest – Target a ser testado	DD-Mês-AAAA	Nome do responsável pelo teste
Cliente	**Projeto**	
Empresa X	Pentest – target a ser testado	

5.1.3 Vulnerabilidades de Nível Baixo

5.1.3.1 URLs com falta de header de prevenção à X-Frame:

O header de prevenção à X-Frame não está presente no website, o que permite a um atacante a incorporação da página em uma página falsa, onde o mesmo pode obter dados e informações sigilosas e pessoais da empresa.
As evidências relacionadas a esta vulnerabilidade estão presentes no Anexo I na última sessão deste relatório.

Solução: Adicionar o header de prevenção à ataques do tipo X-Frame.

5.1.3.2 Cookie não tem flag HttpOnly

Quando um cookie possuir a flag HttpOnly, instrui o navegador que o cookie só pode ser acessado pelo servidor e não por client-side scripts. Esta é uma proteção de segurança importante para cookies de sessão.
As evidências relacionadas a esta vulnerabilidade estão presentes no Anexo I na última sessão deste relatório.

Solução: Adicionar flag HttpOnly para os cookies
https://owasp.org/www-community/HttpOnly

5.1.3.3 Cookie não tem flag Secure

Quando um cookie possuir flag Secure, ela instrui o navegador que o cookie só poderá ser acessado com canais seguros SSL/TLS. Esta é uma proteção de segurança importante para cookies de sessão.
As evidências relacionadas a esta vulnerabilidade estão presentes no Anexo I na última sessão deste relatório.

Solução: Adicionar flag Secure para os cookies
https://owasp.org/www-community/controls/SecureFlag

Anexo Orcamento 01_Atualizado.pdf (0202857) SEI 19.09.02684.0011790/2021-22 / pg. 679

stefaninirafael

Documento	Emitido em	Responsável
Relatório de Pentest – Target a ser testado	DD-Mês-AAAA	Nome do responsável pelo teste
Cliente	**Projeto**	
Empresa X	Pentest – target a ser testado	

5.1.3.4 Cookie de sessão sem expiração

Quando um cookie de sessão não possui tempo de expiração definido, há possibilidade de iniciar ataques de força bruta e de alterações de requisições para o website se utilizando deste recurso.
As evidências relacionadas a esta vulnerabilidade estão presentes no Anexo I na última sessão deste relatório.

Solução: Adicionar tempo de expiração para o cookie de sessão do website.

5.2 Vulnerabilidades do Aplicativo

5.2.1 Vulnerabilidades de Risco Alto

5.2.1.1 Aplicativo com mais permissionamentos que o necessário:

Foi identificado que o aplicativo mobile possui mais permissionamentos que o necessário para seu devido funcionamento. O que permite que o mesmo acesso diversas funções
As evidências relacionadas a esta vulnerabilidade estão presentes no Anexo I na última sessão deste relatório.

Solução: Restringir os acessos do aplicativo para que o mesmo solicite a permissão do usuário para acesso aos dados do aparelho.

5.2.1.2 Aplicativo sem restrições de configurações:

Foi identificado que o aplicativo mobile está com todas as configurações de conexões habilitadas por default o que possibilita o rastreio do aparelho e envio de dados sem quaisquer bloqueios. O que pode ser utilizado por um atacante para envio de requisições falsas e obtenção de informações internas do aplicativo.

Solução: Restringir as configurações do aplicativo para que o mesmo realize as devidas conexões e envio de dados de maneira segura e apenas quando necessário.

Anexo Orcamento 01_Atualizado.pdf (0202857) SEI 19.09.02684.0011790/2021-22 / pg. 680

stefaninirafael

Documento	Emitido em	Responsável
Relatório de Pentest – Target a ser testado	DD-Mês-AAAA	Nome do responsável pelo teste
Cliente	**Projeto**	
Empresa X	Pentest – target a ser testado	

ANEXO A – PENTEST DD DE MÊS DE AAAA

Questionário de escopo de pentest:

Segue abaixo o questionário de escopo de Pentest preenchido pela Empresa X:

Inserir documento preenchido pela Empresa X.

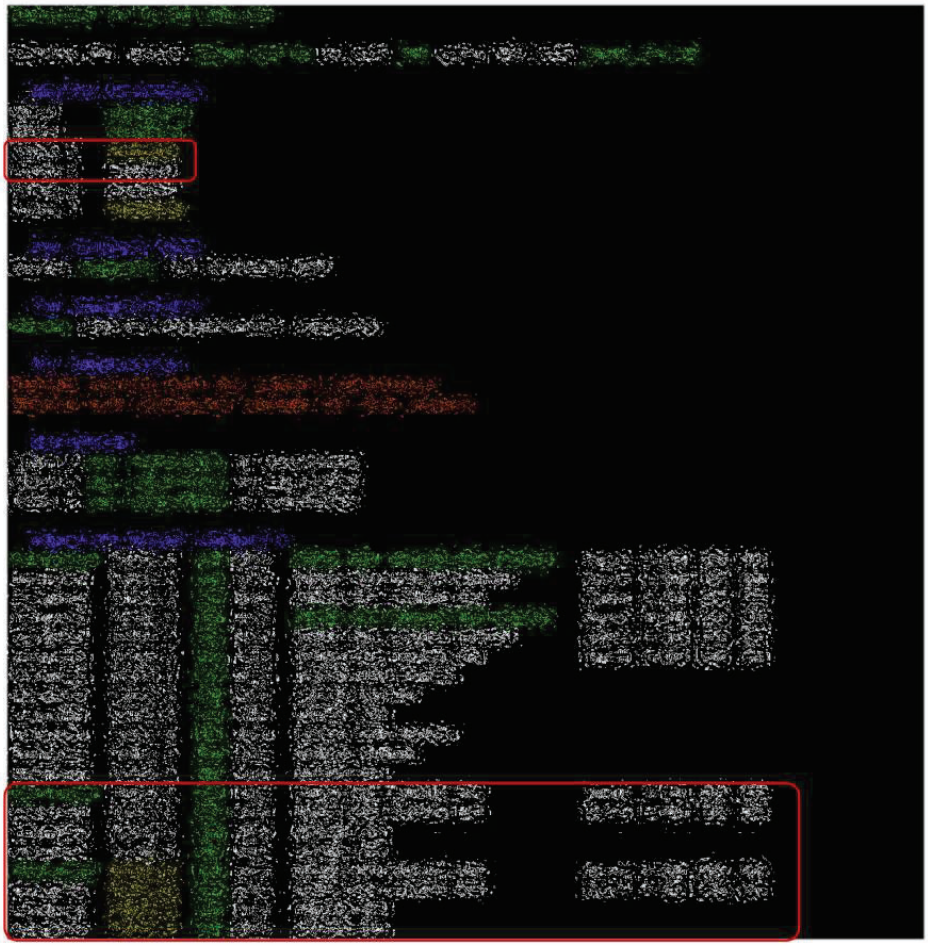
Evidências das vulnerabilidades exploradas:

A seguir seguem as evidências das vulnerabilidades encontradas no ambiente e presentes neste relatório de PenTest. O mesmo foi realizado no período de DD de Mês de AAAA à DD de Mês de AAAA e entregue ao responsável pelo projeto na data de DD de Mês de AAAA.

Anexo Orcamento 01_Atualizado.pdf (0202857) SEI 19.09.02684.0011790/2021-22 / pg. 681

stefaninirafael

Documento	Emitido em	Responsável
Relatório de Pentest – Target a ser testado	DD-Mês-AAAA	Nome do responsável pelo teste
Cliente	**Projeto**	
Empresa X	Pentest – target a ser testado	



Anexo Orcamento 01_Atualizado.pdf (0202857) SEI 19.09.02684.0011790/2021-22 / pg. 682

stefaninirafael

Documento	Emitido em	Responsável
Relatório de Pentest – Target a ser testado	DD-Mês-AAAA	Nome do responsável pelo teste
Cliente	**Projeto**	
Empresa X	Pentest – target a ser testado	



Imagem 2 - Evidência de arquivo configuração do arquivo robots

Anexo Orcamento 01_Atualizado.pdf (0202857) SEI 19.09.02684.0011790/2021-22 / pg. 683

stefaninirafael

Documento	Emitido em	Responsável
Relatório de Pentest – Target a ser testado	DD-Mês-AAAA	Nome do responsável pelo teste
Cliente	**Projeto**	
Empresa X	Pentest – target a ser testado	

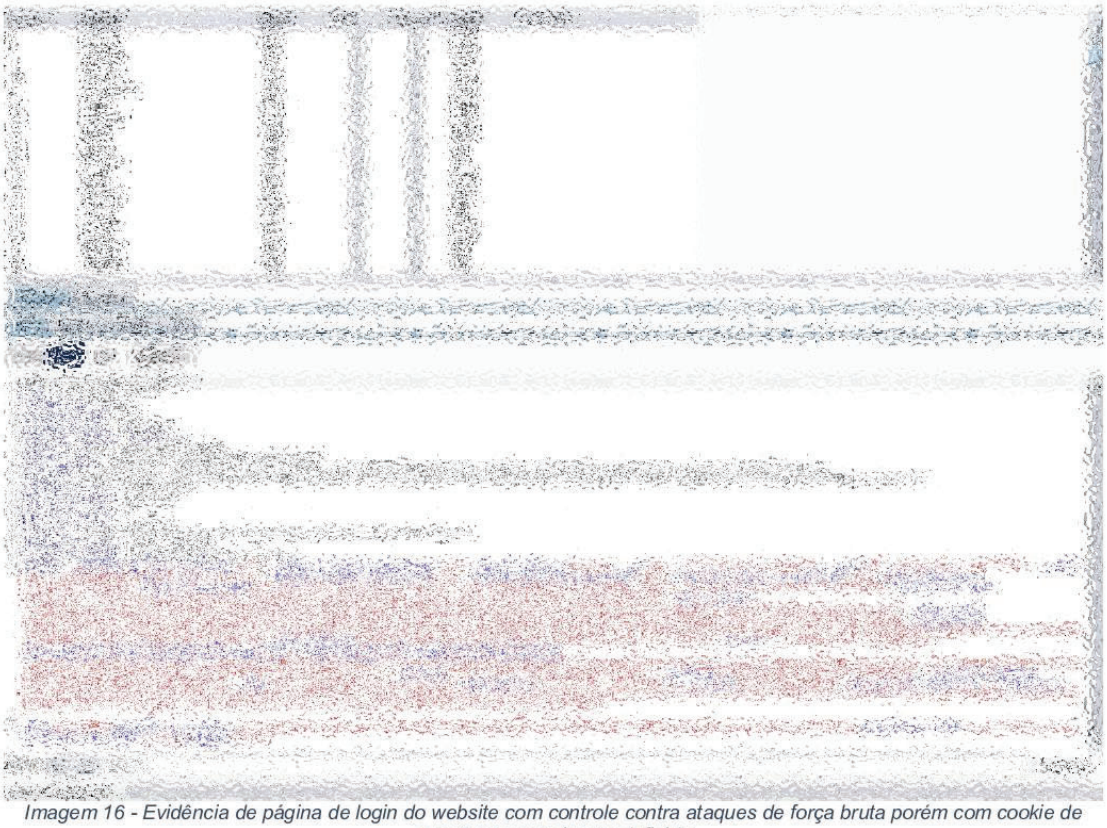


Imagem 16 - Evidência de página de login do website com controle contra ataques de força bruta porém com cookie de sessão sem expiração definida

Anexo Orcamento 01_Atualizado.pdf (0202857) SEI 19.09.02684.0011790/2021-22 / pg. 684

stefaninirafael

Documento	Emitido em	Responsável
Relatório de Pentest – Target a ser testado	DD-Mês-AAAA	Nome do responsável pelo teste
Cliente	**Projeto**	
Empresa X	Pentest – target a ser testado	



Anexo Orcamento 01_Atualizado.pdf (0202857) SEI 19.09.02684.0011790/2021-22 / pg. 685

stefaninirafael

Documento	Emitido em	Responsável
Relatório de Pentest – Target a ser testado	DD-Mês-AAAA	Nome do responsável pelo teste
Cliente	**Projeto**	
Empresa X	Pentest – target a ser testado	



Imagem 19 - Evidência de conflitos de chaves SHA1 no código-fonte do aplicativo



Imagem 20 - Evidência de conflitos de chaves SHA1 no código-fonte do aplicativo

Anexo Orcamento 01_Atualizado.pdf (0202857) SEI 19.09.02684.0011790/2021-22 / pg. 686

IBLISS
DIGITAL SECURITY

MINISTÉRIO PÚBLICO
DO ESTADO DA BAHIA

- Proposta Testes de Invasão
27/09/2021 | Validade: 30 dias

A EMPRESA

A IBLISS, empresa especializada em segurança digital, é referência nacional em desenvolvimento e fornecimento de soluções estratégicas para a proteção de negócios e pessoas.
Fundada em São Paulo em 2009 e formada por especialistas e engenheiros certificados com mais de quinze anos de experiência, a iBLISS tem apoiado empresas 100+ da Exame e Fortune 500 em projetos de Segurança da Informação de alta complexidade, gestão de riscos, diagnósticos, adequação, monitoração e prevenção de ameaças digitais.
Por meio de programas estratégicos de proteção orientado aos objetivos de negócio de cada companhia, a abordagem de atuação da iBLISS possibilita a melhoria contínua da maturidade em segurança com redução de custo.

Posicionamento

A transformação digital tem feito com que a segurança tradicional seja levada a uma nova realidade, que deve levar em consideração o atual cenário de ameaças, em que os ataques cibernéticos têm causado uma série de prejuízos às finanças e à imagem da empresa.
Nossa abordagem é baseada no contexto de cada negócio com o objetivo de reduzir custos com a prevenção de incidentes e perdas e dar apoio à tomada de decisão com base em análises técnicas sempre alinhadas à política corporativa e às melhores práticas de segurança.
A iBLISS gerencia e monitora mais de 100 mil ativos por mês, realizando testes de segurança, consultorias, proteção de aplicações e programas de conscientização. Atuamos nos principais segmentos de mercado, atendendo a requisitos de segurança generalistas e regulamentações específicas, como PCI-DSS, SOX, TISS entre outras.

Missão

Por meio de serviços especializados, pesquisa, desenvolvimento e inovação, apoiar a maturidade e o gerenciamento de riscos de nossos clientes, e contribuir para o crescimento do mercado brasileiro em soluções de segurança da informação.

A EMPRESA

IBLISS DIGITAL SECURITY

+60 Clientes	+100.000	+10.000 horas	+12 Anos	+30%
				
+10 na lista das 100 Maiores Empresas da Exame	Ativos analisados por mês	de testes de segurança por ano	de experiência em Projetos Especiais	Crescimento anual desde 2013

FUNDAÇÃO ABRINQ

Great Place To Work. Certificado 24/02/2020 - 24/02/2021 BRASIL

inovaBra habitat

A EMPRESA

IBLISS DIGITAL SECURITY

Equipe

Formada por profissionais com grande vivência de mercado, nossa equipe possui profundo conhecimento e constante atualização a respeito de técnicas de ataque, novas ameaças e métodos de proteção.
Isso se dá, principalmente, por conta de publicações e participações em comunidades e congressos nacionais e internacionais (DefCon, HITB, OWASP, ToorCon, H2HC, YSTS), além da obtenção de certificações (SANS GIAC, CEH, MCSO, CCNA, CCDA, ITIL, Cobit, ISO 27002, entre outras).



Dados Cadastrais

Razão Social: IBLISS Segurança Digital LTDA.
CNPJ: 10.739.169/0001-11
Endereço: Av. Angélica, 2582 - cj 22 - Higienópolis, São Paulo - SP - Brasil
Representante Legal: Leonardo Cavallari Militelli
E-mail: leonardo.militelli@ibliss.com.br
Ref. Bancárias: Banco Itaú – Ag.: 3052 – C/C: 09668-6

A EMPRESA

IBLISS DIGITAL SECURITY

Empresa com propósito

Programa de responsabilidade social

- Incentivar a navegação saudável
- Inclusão de mulheres em Cyber Segurança

Apoia à comunidade de infosec

- Conferências
- Palestras e colaboração

https://www.ibliss.digital/responsabilidadesocial/

FUNDAÇÃO ABRINQ



NULLBYTE

WOMCY
LATAM Women in Cybersecurity

OWASP

CLIENTES

Varejo e Indústria

viavarejo · 3 Corações · Ajinomoto · Solar Coca-Cola · atech Grupo Embraer

Financeiro e Meios de Pagamento

Itaú · Bradesco · Safra · Banco Máxima · Honda Serviços Financeiros · Santander · CIP · Banco Paulista · ParanáBanco · stone

Saúde

Hypera pharma · novo nordisk · 4BIO · aliar médicos à frente · db Medicina Diagnóstica

Logística

EMBRAPORT · Brasil Terminal Portuário · S.Magalhães Essemaga · sequoia

Telecom e Tecnologia

Telefônica · TIM · Algar · AUTOPASS · LISTO

Serviços

sodexo · livelo · stix · alelo · CVC · Repom · yandeh · involves · acesso digital

Governo e Associações

CIESP · FIESP · UNINOVE Universidade Nove de Julho · Ministério Público Estado da Bahia

IBLISS DIGITAL SECURITY

Construa seu Programa de Segurança da Informação e Privacidade!

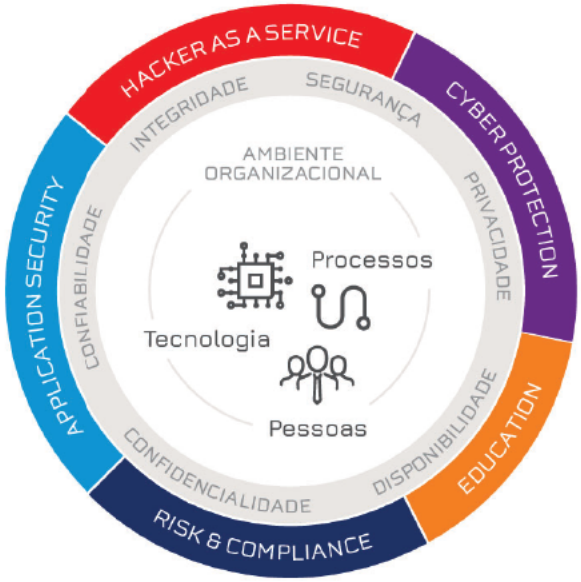


ISO 27001 Certified · GDPR READY · General Data Protection Regulation · LGPD Lei Geral de Proteção de Dados Pessoais · NIST National Institute of Standards and Technology U.S. Department of Commerce · PCI Security Standards Council

OBJETIVO

O objetivo deste trabalho é a realização de serviço de Testes de invasão, proporcionando um melhor direcionamento de seus recursos, através de recomendações detalhadas de medidas de segurança, priorizadas conforme a criticidade dos riscos encontrados.

O IBLISS framework está sempre alinhado ao objetivos e negócio da Organização, baseado nas melhores práticas, normas e frameworks de mercado, analisando Tecnologias, Pessoas e Processos, permitindo identificar o nível de maturidade de Segurança da Informação e consolidando o resultado dentro da solução GAT, como demonstra na imagem abaixo.



HACKER AS A SERVICE

COMPONENTES DA OFERTA

IBLISS DIGITAL SECURITY



1. Análise técnica



2. Relatório de Riscos



3. Suporte a correção e validação

PENETRATION TESTING EXECUTION STANDARD PTES Technical Guidelines

OWASP Open Web Application Security Project

NIST

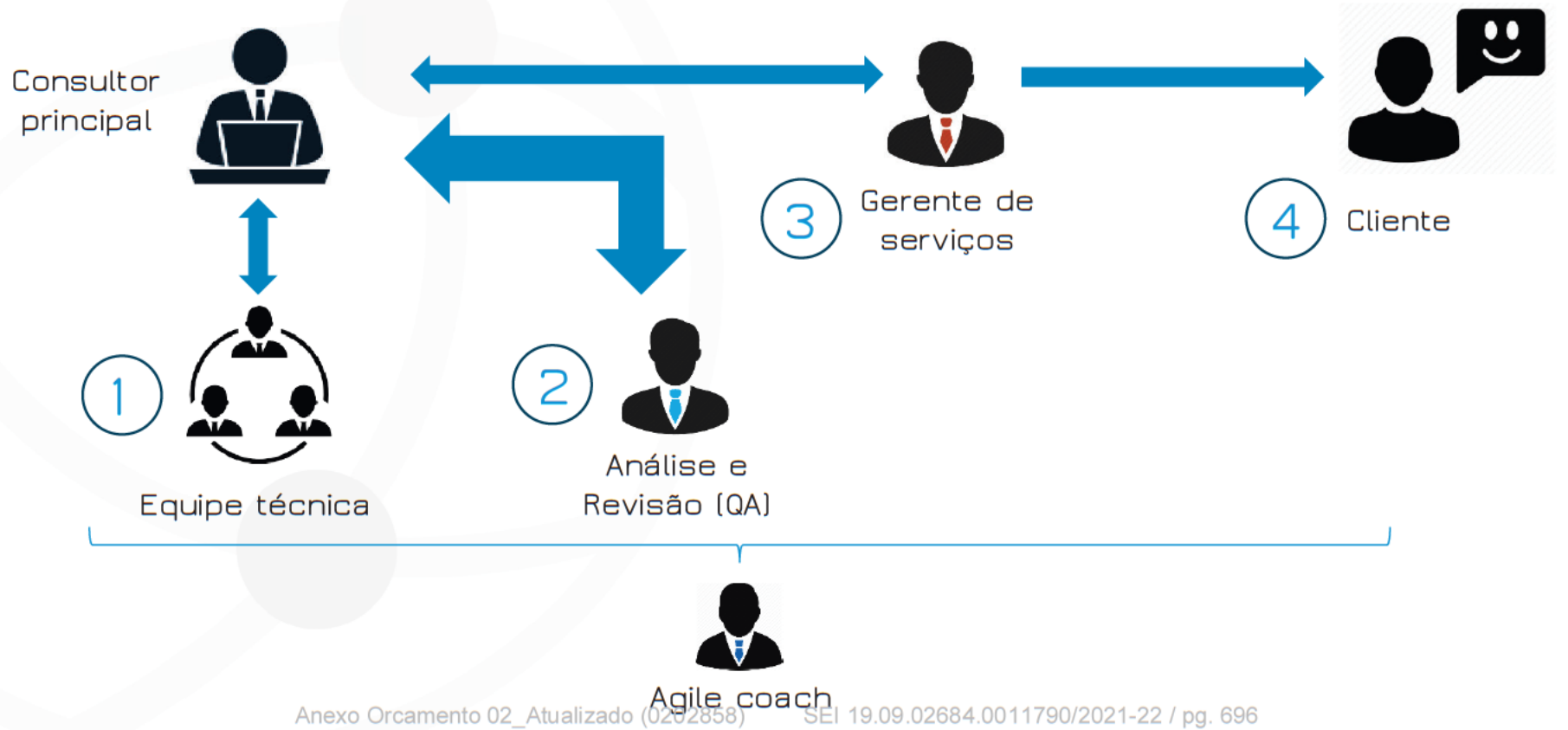
Open Source Security Testing Methodology Manual OSSTMM www.osstmm.org

ISSAF Information Systems Security Assessment Framework www.oissg.org

HACKER AS A SERVICE

PROCESSO DE EXECUÇÃO DO PROJETO

IBLISS DIGITAL SECURITY



HACKER AS A SERVICE

TIPOS DE TESTES

IBLISS DIGITAL SECURITY

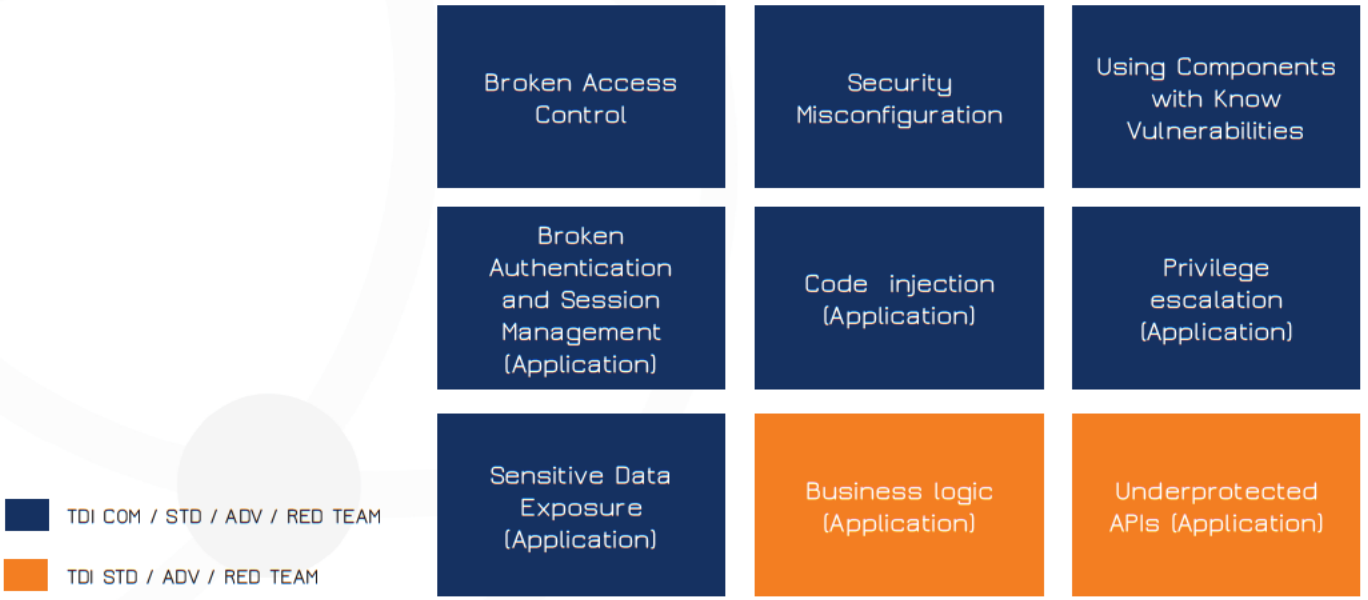
	Teste de Invasão Compliance	Análise de Vulnerabilidades	Teste de Invasão Advanced	Red Team
Objetivo	Testes de segurança em todos os alvos do escopo	Testes de segurança em todos os alvos do escopo	Testes de segurança orientado aos objetivos específicos	Testes de segurança orientado aos objetivos específicos
Execução	Remoto/Local	Remoto/Local	Remoto	Remoto/Local
Scan de vulnerabilidades	√	√	√	√ (se necessário)
Validações de falsos positivos e consolidação de vulnerabilidades	√	√	√	√
Análises manuais*	√		√	√
Exploração da vulnerabilidade e movimentação lateral			√	√
Engenharia social (Phishing, Vishing, SMiShing)				√
Engenharia social (Físico)				√
OSINT - Open Source Intelligence			√	√
Wireless				√

Anexo Orçamento 02_Atualizado (0202858) SEI 19.09.02684.0011799/2021-22 / pg. 697

HAAS - MODALIDADES

OPCÕES PARA EXECUÇÃO DO TESTE

Análises manuais - para as modalidades que possuem análises manuais os seguintes testes se aplicam



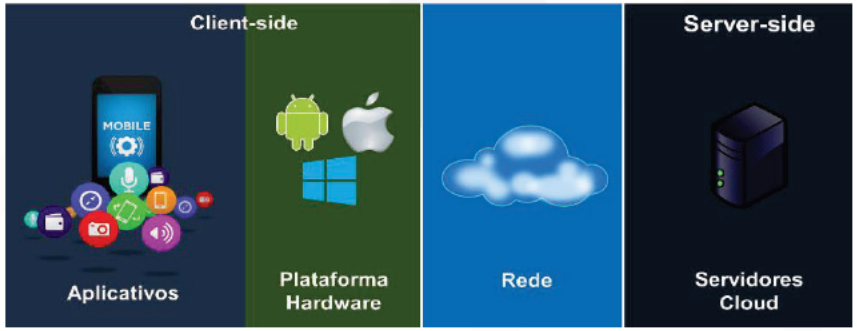
METODOLOGIA DE ANÁLISE

INFRAESTRUTURA / APP WEB

- Broken Access Control
- Information Gathering:
- Network Discovery / Network enumeration
- Network Port and Service Identification
- Password Cracking
- Privilege escalation
- Security Misconfiguration
- Sensitive Data Exposure
- Using Components with Known Vulnerabilities
- Vulnerability analysis / Scanning
- Broken Access Control (Authenticated users controls, Privilege escalation)
- Broken Authentication (Authentication and session management)
- Business logic
- Cross-Site Scripting (XSS)
- Data Validation Testing:
- Information Gathering:
- Insecure Deserialization
- Insufficient Logging&Monitoring
- Injection
- Underprotected APIs (Applications integration)
- Using Components with Known Vulnerabilities
- Web Services Testing:
- XML External Entities (XXE)

METODOLOGIA DE ANÁLISE

APP MOBILE



Análise de aplicação mobile

- Na análise de aplicativos mobile realizamos análise técnicas baseadas na seguinte metodologia

Client-side:

- Autenticação insegura
- Autorização insegura
- Armazenamento inseguro de dados
- Code tampering
- Criptografia insuficiente
- Engenharia reversa
- Funcionalidades externas, utilização de recursos externos a plataforma
- Uso de plataforma imprópria

Comunicação client-side e server-side

- Criptografia insuficiente
- Comunicação insegura

Server-side (Análise remota)

- Code injection
- Análise externa da infraestrutura

HAAS - MODALIDADES

OPCÕES PARA EXECUÇÃO DO TESTE

IBLISS DIGITAL SECURITY

	Acesso a Informações	Credenciais	URL/IP	Benefícios
White-Box	Sim	Sim	Sim	A partir das informações recebidas, pode ser feito um teste direcionado a aplicação, ao sistema operacional e dispositivos de rede. Obtendo melhores resultados na exploração das vulnerabilidades e falhas.
Grey-Box	Não	Sim	Sim	Para este teste é fornecido parcialmente informações sobre o ambiente analisado.
Black-Box	Não	Não	Não	O benefício deste teste é aplicar um ataque real, onde é pressuposto que um usuário mal intencionado não terá nenhuma informação sobre a aplicação.

HAAS - FERRAMENTAS

- Plataforma GAT - Para gestão de vulnerabilidades
- NMAP -Varredura de Portas;
- Maltego e Ferramenta própria - Levantamento de informações;
- Tenable Nessus Professional Feed - Levantamento de vulnerabilidades;
- W3AF - Levantamento de vulnerabilidades;
- Metasploit Framework e Exploit Tree - Exploração de vulnerabilidades;
- Acunetix - Avaliação das aplicações Web;
- Burp Professional Edtion - Avaliação das aplicações Web;
- SQL Map - Avaliação de Aplicações e Banco de Dados;
- Ferramentas OWASP - Avaliação das aplicações Web;
- Mobile Security Framework - Avaliação das aplicações Mobile;
- Entre outras ferramentas desenvolvidas internamente, sendo algumas publicada em:
  - https://github.com/iBLISSLabs1

ESCOPO DO PROJETO

O escopo para este projeto foi definido nos seguintes parâmetros:

- **Periodicidade:** Pontual
- **Tipo de teste:** Teste de invasão Advanced Black box em plataforma de voto eletrônico

Pentest

Aplicação WEB em BLACK-BOX – Plataforma de voto eletrônico conforme documento de especificação técnica

- **Reteste e suporte IBLISS para correções:** 60 dias após a entrega dos resultados
- **Acesso a plataforma GAT** durante 60 dias após a entrega dos resultados

EXECUÇÃO

- Todas as atividades e serviços serão executadas em horário comercial.
- O cliente deverá informar previamente os pontos de contatos principais e secundários para o acompanhamento desse contrato.
- Toda solicitação de um novo serviço deverá ser realizada ao Gerente Comercial da IBLISS responsável pelo acompanhamento do contrato.
- As equipes do Cliente e IBLISS deverão alinhar previamente qual o escopo necessário para cada atividade.
- O Cliente deverá informar a IBLISS qual o objetivo para cada atividade solicitada.
- A IBLISS informará ao Cliente qual o esforço necessário com relação a tempo e recursos disponíveis para a execução de cada atividade.
- O Cliente deverá aprovar previamente a realização das atividades considerando a quantidade de horas definidas pela IBLISS.
- Haverá gerenciamento constante das atividades, com objetivo de manter as partes informadas, resolver dificuldades e definir a necessidade de maior número de horas.
- Sempre que julgar necessário a IBLISS atuará de forma consultiva informando ao Cliente quais são as melhores práticas há serem estabelecidas para cada atividade.
- Vulnerabilidades detectadas:
    - Caso detectadas vulnerabilidades críticas, estas serão reportadas imediatamente por meio de relatórios emergenciais;
    - Caso seja identificada alguma vulnerabilidade que possa ocasionar a negação de serviço (DoS), a qual não faz parte do escopo, esta será informada ao responsável do cliente para que então seja tomada a decisão apropriada sobre a execução do teste.

CRONOGRAMA

De acordo com o escopo definido para o projeto, as atividades estão agrupadas em um cronograma que dará a adequada percepção e visão das fases, marcos de controle e esforço estimado para sua execução, a fim de permitir o acompanhamento do projeto.

Os trabalhos poderão ser iniciados em até 10 dias para serviços remotos e 30 dias para serviços in-loco a partir da assinatura deste contrato, mediante verificação de disponibilidade de equipe.

O cliente poderá utilizar o serviço contratado em até 6 meses após a assinatura do contrato, após esse prazo as condições do contrato podem ser revistas.

SUPORTE A CORREÇÃO DE VULNERABILIDADES E RETESTE

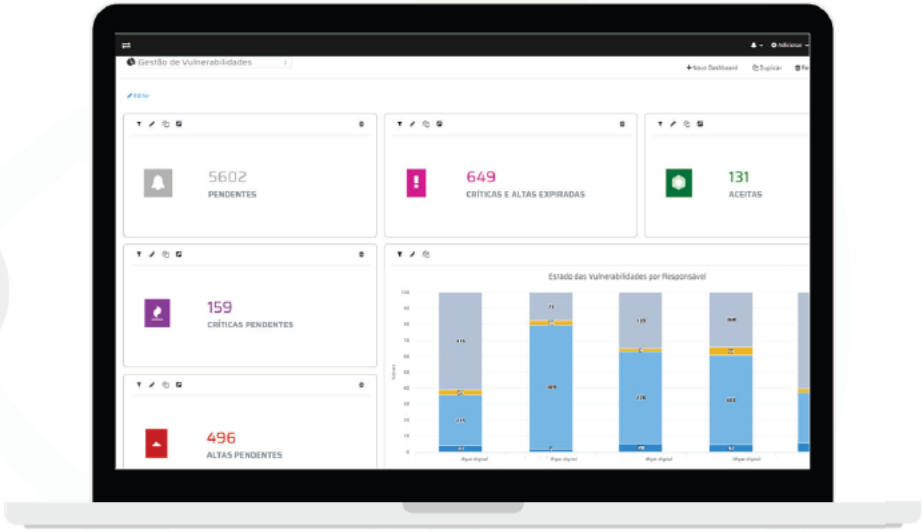
Após a geração dos relatórios finais e apresentação dos mesmos, é oferecido suporte às equipes técnicas para implementação das correções. Este apoio poderá ser utilizado durante 120 dias após a entrega dos testes.

O cliente também poderá solicitar em até 60 dias após a entrega do projeto o reteste para validação da correção das vulnerabilidades encontradas.

O suporte à correção será oferecido por nossa plataforma de suporte, por meio do e-mail suporte@ibliss.com.br

GAT - PLATAFORMA

IBLISS DIGITAL SECURITY



94%

Aumento do nível de Segurança Digital

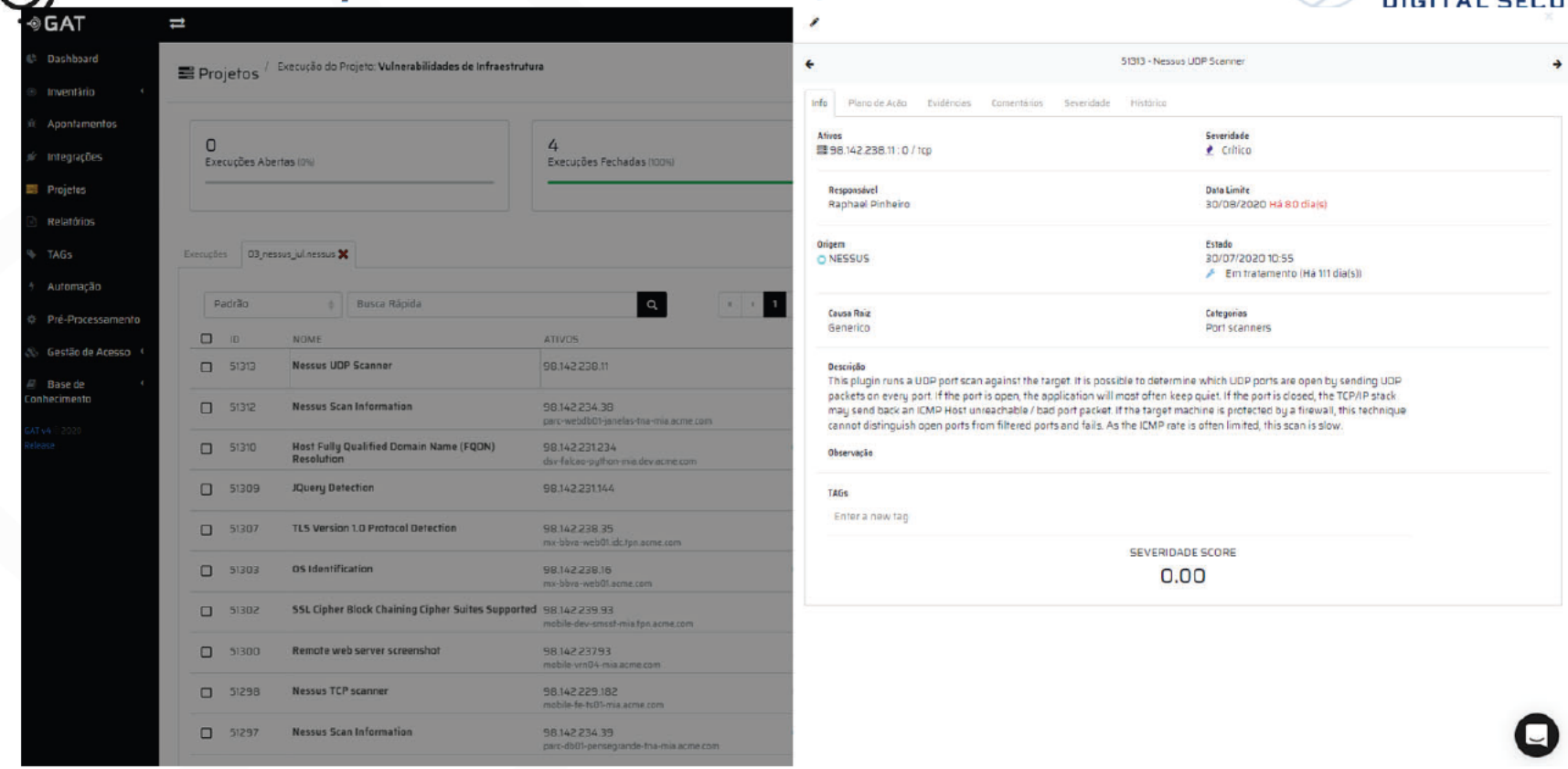
55%

Aumento da produtividade de analistas de TI / SI

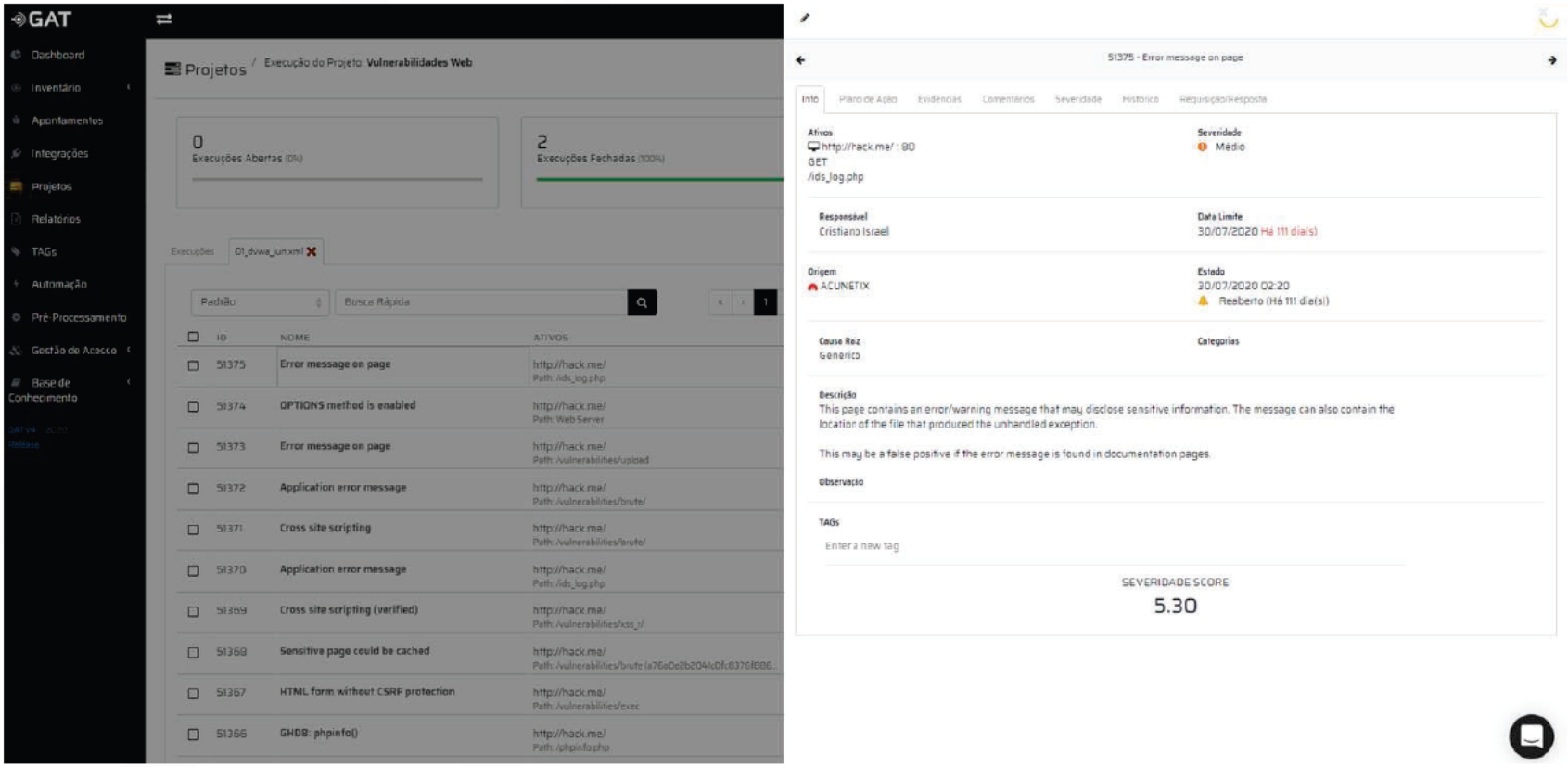
O: resultados serão disponibilizados na plataforma GAT pelo período de 60 dias, para até 02 usuários. Essa plataforma facilita o processo de correção dos pontos encontrados durante os testes, além de facilitar o compartilhamento dos resultados dos testes com as equipes responsáveis pelos ativos. As principais características são:

- Acompanhamento das correções;
- Fácil identificação dos ambientes mais críticos;
- Obtenção de maiores informações sobre cada vulnerabilidade;

ESTABELEÇA E MENSURE KPI's, KRI's e SLA's

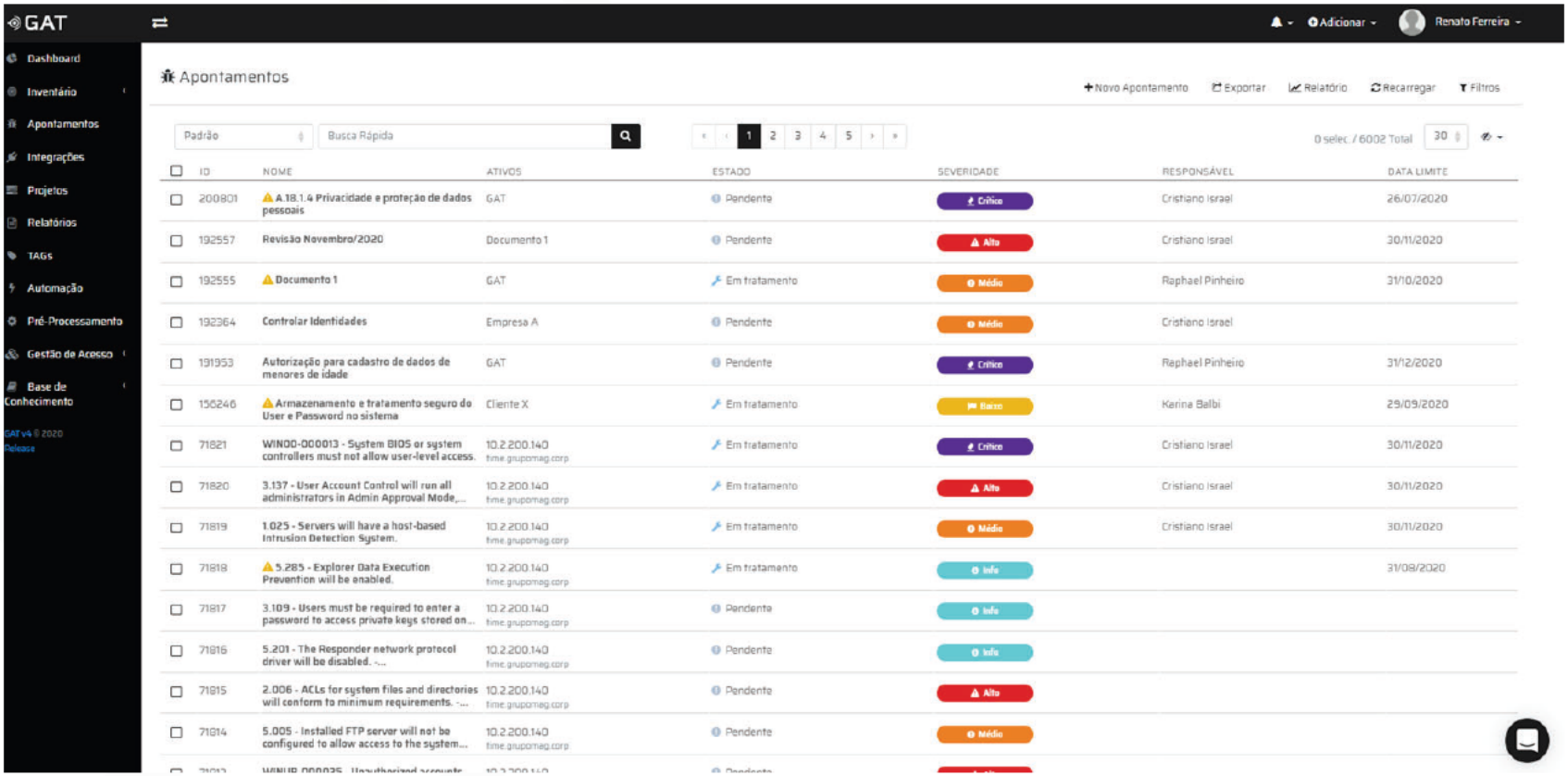


ESTABELEÇA E MENSURE KPI's, KRI's e SLA's



ESTABELEÇA E MENSURE KPI's, KRI's e SLA's

IBLISS DIGITAL SECURITY



Apontamentos

LIMITAÇÕES E RESPONSABILIDADES

Estão fora do escopo do projeto

- Realização de testes que tenham por objetivo causar indisponibilidade de serviços ou ativos de forma externa (DDoS, DoS, flood, etc);
- Análise local dos equipamentos, como, por exemplo, levantar e analisar as regras de firewall ou validar o uso de procedimentos de hardening nos servidores ou serviços;
- Avaliação de controles disponíveis somente do lado do servidor, bem como validação de regras de negócio;
- Execução da correção e implantação de soluções.
- URL´s e sistemas que não estejam dentro do especificado nessa proposta e de acordo com acordado no projeto.

Limitação

- A Contratante deve estar ciente de que serão tomadas todas as providências para que o teste não provoque indisponibilidade ou impacto na aplicação. No entanto, mesmo com os maiores cuidados aplicados, poderá haver algum comportamento não previsto, podendo afetar a estabilidade da aplicação. Como as condições de segurança dos equipamentos e aplicações são desconhecidas, reações inesperadas podem acontecer, dessa forma recomenda-se a definição de um ponto de contato de um técnico de suporte do cliente, mas a IBLISS irá apoiar todo processo até o restabelecimento do mesmo.

RECURSOS ALOCADOS

Sugerimos a constituição da seguinte equipe de projeto:

Do lado da IBLISS:

•1 consultor sênior, que executará os trabalhos definidos nesta proposta;

•Equipe de pentesters que dão apoio técnico ao consultor principal;

•1 gerente de projeto, que assegurará a boa execução dos trabalhos reportados nesta proposta, assim como servirá de ponto de contato privilegiado entre a equipe e o cliente;

•1 gerente de QA, que irá revisar todas as entregas deste projeto.

Do lado do cliente:

•1 responsável pelo acompanhamento da execução dos trabalhos do projeto e que servirá de ponto de contato.

CONDIÇÕES COMERCIAIS

Item	Atividades	Tempo execução	Valor R$
Hacker as a Service (HaaS)	Teste de invasão Advanced Black –Box Aplicação WEB	40 horas	R$12.000,00

- Valores expressos em Reais (R$) com base em Julho de 2021 e válidos por 30 (trinta) dias a contar da emissão desta proposta;
- O pagamento deverá ser realizado em parcela única 30 dias após a emissão da nota fiscal após o aceite
- Custos de deslocamento não estão inclusos no valor da proposta;
- Tributos já inclusos no valor apresentado.

IBLISS
DIGITAL SECURITY

Fernanda Olivato

Sales Account Manager

Fernanda.olivato@ibliss.com.br
+ 55 11 96300-7203
+ 55 11 3255-3926

Ibliss.com.br
Avenida Angélica, 2582 - Cj. 22
Higienópolis - São Paulo - Brasil
#porumasociedademaissegura

RE: Solicitação de orçamento - Pentest VotDigital

Iaçanã Lima de Jesus Carneiro <iassa@mpba.mp.br>
Ter, 28/09/2021 10:10

Para: Emilia Pitanga Sampaio Mettig <emilia.mettig@telefonica.com>
Cc: Lival Chagas Estrela <lival.estrela@telefonica.com>

Bom dia!!

Emilia, conforme conversamos a pouco, nós precisamos da mesma proposta com a data de validade atualizada. Como nosso processo é lento as propostas acabaram vencendo e nosso Jurídico, para dar prosseguimento aos finalmentws, nos devolveu o processo solicitando a atualização das validades de todas as propostas.

Já contamos com o entendimento e a ajuda de todos os outros participantes, a VIVO enxerga algum problema em nossa solicitação?! Caso positivo, solicito que nos posicione, pois precisamos dar prosseguimento ao processo que deverá começar em 01/10.

Grato pela atenção de sempre, estamos no aguardo.

Cordialmente
Iaçanã L. J. Carneiro | Tel. (71) 3103-0212 / 0214
CASI - Coordenação de Assessoramento em Segurança da informação
http://www.mpba.mp.br

De: Iaçanã Lima de Jesus Carneiro <iassa@mpba.mp.br>
Enviado: sexta-feira, 24 de setembro de 2021 10:47
Para: Emilia Pitanga Sampaio Mettig <emilia.mettig@telefonica.com>
Cc: Lival Chagas Estrela <lival.estrela@telefonica.com>
Assunto: RE: Solicitação de orçamento - Pentest VotDigital

Emilia, bom dia!

Tem alguma resposta sobre a atualização do vencimento da proposta?!

Grato.

Cordialmente

Anexo Emails_Enviado_VIVO (0202861) SEI 19.09.02684.0011790/2021-22 / pg. 715

Iaçanã L. J. Carneiro | Tel. (71) 3103-0212 / 0214
CASI - Coordenação de Assessoramento em Segurança da informação
http://www.mpba.mp.br

De: Emilia Pitanga Sampaio Mettig <emilia.mettig@telefonica.com>
Enviado: segunda-feira, 20 de setembro de 2021 20:06
Para: Iaçanã Lima de Jesus Carneiro <iassa@mpba.mp.br>
Cc: Lival Chagas Estrela <lival.estrela@telefonica.com>
Assunto: RES: Solicitação de orçamento - Pentest VotDigital

Iaçanã,

Tudo bem? Solicitei ao pre-vendas responsável a validação do valores e autorização para prorrogação do prazo da proposta.

Assim que tiver essa confirmação eu te retorno.

Abs.,

Emília Pitanga Sampaio Mettig
Diretoria de Governo | Gerencia Governo FSP
Gerente de Negocios – Especialista Governo
Tel.: (071) 99980-2026
Rua Silveira Martins, nº1036, Módulo 6, Cabula,
Salvador (BA), Cep.:41150-000
E-mail: emilia.mettig@telefonica.com



Este mensagem e seus anexos se dirigem unicamente ao seu destinatário e são para seu uso exclusivo, pois podem conter informação privilegiada ou confidencial. Se você não é o destinatário indicado, notificamos que a leitura, utilização, divulgação e/ou cópia sem autorização do conteúdo desta email pode estar proibida em virtude da legislação vigente. Se recebeu esta mensagem por engano, pedimos que comunique imediatamente ao remitente e exclua esta mensagem.

De: Iaçanã Lima de Jesus Carneiro <iassa@mpba.mp.br>
Enviada em: segunda-feira, 20 de setembro de 2021 15:50
Para: Emilia Pitanga Sampaio Mettig <emilia.mettig@telefonica.com>
Cc: Lival Chagas Estrela <lival.estrela@telefonica.com>
Assunto: RE: Solicitação de orçamento - Pentest VotDigital

Emilia, boa tarde!

Anexo Emails_Enviado_VIVO (0202861) SEI 19.09.02684.0011790/2021-22 / pg. 716

Precisamos do favor de atualizar a data desta proposta, devido ao tempo de trâmitação a data de validade expirou.

Certo do seu entendimento, agradecemos a atenção.

Cordialmente
Iaçanã L. J. Carneiro | Tel. (71) 3103-0212 / 0214
CASI - Coordenação de Assessoramento em Segurança da informação
http://www.mpba.mp.br

De: Emilia Pitanga Sampaio Mettig <emilia.mettig@telefonica.com>
Enviado: terça-feira, 3 de agosto de 2021 11:11
Para: Iaçanã Lima de Jesus Carneiro <iassa@mpba.mp.br>
Cc: Lival Chagas Estrela <lival.estrela@telefonica.com>
Assunto: RES: Solicitação de orçamento - Pentest VotDigital

Iaçanã,

Bom dia! Segue em anexo proposta atualizada conforme solicitado.

Ats.,

Emília Pitanga Sampaio Mettig
Diretoria de Governo | Gerencia Governo FSP
Gerente de Negocios – Especialista Governo
Tel.: (071) 99980-2026
Rua Silveira Martins, nº1036, Módulo 6, Cabula,
Salvador (BA), Cep.:41150-000
E-mail: emilia.mettig@telefonica.com



Esta mensagem e seus anexos se dirigem unicamente ao seu destinatário e são para seu uso exclusivo, pois podem conter informação privilegiada ou confidencial. Se você não é o destinatário indicado, notificamos que a leitura, utilização, divulgação e/ou cópia sem autorização do conteúdo desta email pode estar proibida em virtude da legislação vigente. Se recebeu esta mensagem por engano, pedimos que comunique imediatamente ao remitente e exclua esta mensagem.

De: Iaçanã Lima de Jesus Carneiro <iassa@mpba.mp.br>
Enviada em: terça-feira, 3 de agosto de 2021 09:43
Para: Emilia Pitanga Sampaio Mettig <emilia.mettig@telefonica.com>
Cc: Lival Chagas Estrela <lival.estrela@telefonica.com>
Assunto: RE: Solicitação de orçamento - Pentest VotDigital

Anexo Emails_Enviado_VIVO (0202861) SEI 19.09.02684.0011790/2021-22 / pg. 717

Bom dia a todos!

@Emilia Pitanga Sampaio Mettig, continuamos aguardando.

Grato pela atenção e ajuda.

Cordialmente
Iaçanã L. J. Carneiro | Tel. (71) 3103-0212 / 0214
CASI - Coordenação de Assessoramento em Segurança da informação
http://www.mpba.mp.br

De: Iaçanã Lima de Jesus Carneiro <iassa@mpba.mp.br>
Enviado: segunda-feira, 2 de agosto de 2021 10:35
Para: Emilia Pitanga Sampaio Mettig <emilia.mettig@telefonica.com>
Cc: Lival Chagas Estrela <lival.estrela@telefonica.com>
Assunto: RE: Solicitação de orçamento - Pentest VotDigital

Emilia, bom dia!

Conforme nos falamos a pouco, nossa área de Contratos solicitou que a data de vencimento deste orçamento fosse atualizada, poderia nos fazer esse favor e atualizar por mais 30 dias?!

Agradeço pela ajuda de sempre.

Cordialmente
Iaçanã L. J. Carneiro | Tel. (71) 3103-0212 / 0214
CASI - Coordenação de Assessoramento em Segurança da informação
http://www.mpba.mp.br

De: Emilia Pitanga Sampaio Mettig <emilia.mettig@telefonica.com>
Enviado: terça-feira, 20 de julho de 2021 17:08
Para: Iaçanã Lima de Jesus Carneiro <iassa@mpba.mp.br>

Anexo Emails_Enviado_VIVO (0202861) SEI 19.09.02684.0011790/2021-22 / pg. 718

Cc: Lival Chagas Estrela <lival.estrela@telefonica.com>
Assunto: RES: Solicitação de orçamento - Pentest VotDigital

Iaçanã,

Boa Tarde! Conforme nossa conversa segue em anexo a Proposta da Telefônica para essa demanda.

Desde já agradeço mais uma vez a oportunidade.

Ats.,

Emília Pitanga Sampaio Mettig
Diretoria de Governo | Gerencia Governo FSP
Gerente de Negocios – Especialista Governo
Tel.: (071) 99980-2026
Rua Silveira Martins, nº1036, Módulo 6, Cabula,
Salvador (BA), Cep.:41150-000
E-mail: emilia.mettig@telefonica.com

vivo EMPRESAS
Esta mensagem e seus anexos se dirigem unicamente ao seu destinatário e são para seu uso exclusivo, pois podem conter informação privilegiada ou confidencial. Se você não é o destinatário indicado, notificamos que a leitura, utilização, divulgação e/ou cópia sem autorização do conteúdo desta email pode estar proibida em virtude da legislação vigente. Se recebeu esta mensagem por engano, pedimos que comunique imediatamente ao remetente e exclua esta mensagem.

De: Emilia Pitanga Sampaio Mettig
Enviada em: segunda-feira, 19 de julho de 2021 15:47
Para: Iaçanã Lima de Jesus Carneiro <iassa@mpba.mp.br>
Assunto: RES: Solicitação de orçamento - Pentest VotDigital

Iaçanã.

Boa Tarde! Conforme conversamos via zap na sexta-feira, apresentaremos a nossa proposta final amanhã (dia 20/07) sem falta.

Desde já agradeço a oportunidade.

Ats.,

Emília Pitanga Sampaio Mettig
Diretoria de Governo | Gerencia Governo FSP
Gerente de Negocios – Especialista Governo
Tel.: (071) 99980-2026

Anexo Emails_Enviado_VIVO (0202861) SEI 19.09.02684.0011790/2021-22 / pg. 719

Rua Silveira Martins, nº1036, Módulo 6, Cabula,
Salvador (BA), Cep.:41150-000
E-mail: emilia.mettig@telefonica.com

vivo EMPRESAS

Esta mensagem e seus anexos se dirigem unicamente ao seu destinatário e são para seu uso exclusivo, pois podem conter informação privilegiada ou confidencial. Se você não é o destinatário indicado, notificamos que a leitura, utilização, divulgação e/ou cópia sem autorização do conteúdo desde email pode estar proibida em virtude da legislação vigente. Se recebeu esta mensagem por engano, pedimos que comunique imediatamente ao remetente e exclua essa mensagem.

De: Iaçanã Lima de Jesus Carneiro <iassa@mpba.mp.br>
Enviada em: segunda-feira, 19 de julho de 2021 09:59
Para: Emilia Pitanga Sampaio Mettig <emilia.mettig@telefonica.com>
Assunto: RE: Solicitação de orçamento - Pentest VotDigital

Bom dia,

Conforme último contato estamos aguardando a proposta para hoje.

No aguardo.

Grato.

Cordialmente
Iaçanã L. J. Carneiro | Tel. (71) 3103-0212 / 0214
CASI - Coordenação de Assessoramento em Segurança da informação
http://www.mpba.mp.br

De: Emilia Pitanga Sampaio Mettig <emilia.mettig@telefonica.com>
Enviado: quinta-feira, 15 de julho de 2021 19:33
Para: Iaçanã Lima de Jesus Carneiro <iassa@mpba.mp.br>
Assunto: RES: Solicitação de orçamento - Pentest VotDigital

Iaçanã,

Olá! Voltei de férias hoje. Vou verificar e te retorno amanhã sem falta.

Abs.,

Anexo Emails_Enviado_VIVO (0202861) SEI 19.09.02684.0011790/2021-22 / pg. 720

Emília Pitanga Sampaio Mettig
Diretoria de Governo | Gerencia Governo FSP
Gerente de Negocios – Especialista Governo
Tel.: (071) 99980-2026
Rua Silveira Martins, nº1036, Módulo 6, Cabula,
Salvador (BA), Cep.:41150-000
E-mail: emilia.mettig@telefonica.com



Esta mensagem e seus anexos se dirigem unicamente ao seu destinatário e são para seu uso exclusivo, pois podem conter informação privilegiada ou confidencial. Se você não é o destinatário indicado, notificamos que a leitura, utilização, divulgação e/ou cópia sem autorização do conteúdo deste email pode estar proibida em virtude da legislação vigente. Se recebeu esta mensagem por engano, pedimos que comunique imediatamente ao remetente e exclua essa mensagem.

De: Iaçanã Lima de Jesus Carneiro <iassa@mpba.mp.br>
Enviada em: quarta-feira, 14 de julho de 2021 09:44
Para: Iaçanã Lima de Jesus Carneiro <iassa@mpba.mp.br>
Assunto: RE: Solicitação de orçamento - Pentest VotDigital

Bom dia a todos,

O motivo do nosso contato é para verificar como está nossa solicitação de orçamento, pois precisamos passar feedback ao nosso gestor. Nossa preocupação se dá devido a lentidão do nosso processo de compra.

Grato pela atenção de todos.

Cordialmente
Iaçanã L. J. Carneiro | Tel. (71) 3103-0212 / 0214
CASI - Coordenação de Assessoramento em Segurança da informação
http://www.mpba.mp.br

De: Iaçanã Lima de Jesus Carneiro <iassa@mpba.mp.br>
Enviado: quinta-feira, 1 de julho de 2021 11:11
Para: Iaçanã Lima de Jesus Carneiro <iassa@mpba.mp.br>
Assunto: Solicitação de orçamento - Pentest VotDigital

Prezado(a)s, bom dia!

Anexo Emails_Enviado_VIVO (0202861) SEI 19.09.02684.0011790/2021-22 / pg. 721

Conforme e-mail anterior segue em anexo as especificações detalhadas com as correções que posicionamos previamente. Estamos enviando em formato .DOCX para que em caso de dúvidas apontem no mesmo documento em forma de comentários.

Está contratação, a principio, deverá vir termo em setembro para que os testes sejam realizados no mês de outubro, ma podem ocorrer mudanças. Por termos um processo de contratação lento, solicitamos que nos respondam com uma certa brevidade para vencermos essa demanda em tempo hábil.

Qualquer dúvida estamos a disposição

Cordialmente
Iaçanã L. J. Carneiro | Tel. (71) 3103-0212 / 0214
CASI - Coordenação de Assessoramento em Segurança da informação
http://www.mpba.mp.br

Este mensaje y sus adjuntos se dirigen exclusivamente a su destinatario, puede contener información privilegiada o confidencial y es para uso exclusivo de la persona o entidad de destino. Si no es usted. el destinatario indicado, queda notificado de que la lectura, utilización, divulgación y/o copia sin autorización puede estar prohibida en virtud de la legislación vigente. Si ha recibido este mensaje por error, le rogamos que nos lo comunique inmediatamente por esta misma vía y proceda a su destrucción.

The information contained in this transmission is privileged and confidential information intended only for the use of the individual or entity named above. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you have received this transmission in error, do not read it. Please immediately reply to the sender that you have received this communication in error and then delete it.

Esta mensagem e seus anexos se dirigem exclusivamente ao seu destinatário, pode conter informação privilegiada ou confidencial e é para uso exclusivo da pessoa ou entidade de destino. Se não é vossa senhoria o destinatário indicado, fica notificado de que a leitura, utilização, divulgação e/ou cópia sem autorização pode estar proibida em virtude da legislação vigente. Se recebeu esta mensagem por erro, rogamos-lhe que nos o comunique imediatamente por esta mesma via e proceda a sua destruição

---

Este mensaje y sus adjuntos se dirigen exclusivamente a su destinatario, puede contener información privilegiada o confidencial y es para uso exclusivo de la persona o entidad de destino. Si no es usted. el destinatario indicado, queda notificado de que la lectura, utilización, divulgación y/o copia sin autorización puede estar prohibida en virtud de la legislación vigente. Si ha recibido este mensaje por error, le rogamos que nos lo comunique inmediatamente por esta misma vía y proceda a su destrucción.

The information contained in this transmission is privileged and confidential information intended only for the use of the individual or entity named above. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you have received this transmission in error, do not read it. Please immediately reply to the sender that you have received this communication in error and then delete it.

Anexo Emails_Enviado_VIVO (0202861) SEI 19.09.02684.0011790/2021-22 / pg. 722

Esta mensagem e seus anexos se dirigem exclusivamente ao seu destinatário, pode conter informação privilegiada ou confidencial e é para uso exclusivo da pessoa ou entidade de destino. Se não é vossa senhoria o destinatário indicado, fica notificado de que a leitura, utilização, divulgação e/ou cópia sem autorização pode estar proibida em virtude da legislação vigente. Se recebeu esta mensagem por erro, rogamos-lhe que nos o comunique imediatamente por esta mesma via e proceda a sua destruição

---

Este mensaje y sus adjuntos se dirigen exclusivamente a su destinatario, puede contener información privilegiada o confidencial y es para uso exclusivo de la persona o entidad de destino. Si no es usted. el destinatario indicado, queda notificado de que la lectura, utilización, divulgación y/o copia sin autorización puede estar prohibida en virtud de la legislación vigente. Si ha recibido este mensaje por error, le rogamos que nos lo comunique inmediatamente por esta misma vía y proceda a su destrucción.

The information contained in this transmission is privileged and confidential information intended only for the use of the individual or entity named above. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you have received this transmission in error, do not read it. Please immediately reply to the sender that you have received this communication in error and then delete it.

Esta mensagem e seus anexos se dirigem exclusivamente ao seu destinatário, pode conter informação privilegiada ou confidencial e é para uso exclusivo da pessoa ou entidade de destino. Se não é vossa senhoria o destinatário indicado, fica notificado de que a leitura, utilização, divulgação e/ou cópia sem autorização pode estar proibida em virtude da legislação vigente. Se recebeu esta mensagem por erro, rogamos-lhe que nos o comunique imediatamente por esta mesma via e proceda a sua destruição

---

Este mensaje y sus adjuntos se dirigen exclusivamente a su destinatario, puede contener información privilegiada o confidencial y es para uso exclusivo de la persona o entidad de destino. Si no es usted. el destinatario indicado, queda notificado de que la lectura, utilización, divulgación y/o copia sin autorización puede estar prohibida en virtud de la legislación vigente. Si ha recibido este mensaje por error, le rogamos que nos lo comunique inmediatamente por esta misma vía y proceda a su destrucción.

The information contained in this transmission is privileged and confidential information intended only for the use of the individual or entity named above. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you have received this transmission in error, do not read it. Please immediately reply to the sender that you have received this communication in error and then delete it.

Esta mensagem e seus anexos se dirigem exclusivamente ao seu destinatário, pode conter informação privilegiada ou confidencial e é para uso exclusivo da pessoa ou entidade de destino. Se não é vossa senhoria o destinatário indicado, fica notificado de que a leitura, utilização, divulgação e/ou cópia sem autorização pode estar proibida em virtude da legislação vigente. Se recebeu esta mensagem por erro, rogamos-lhe que nos o comunique imediatamente por esta mesma via e proceda a sua destruição

Anexo Emails_Enviado_VIVO (0202861) SEI 19.09.02684.0011790/2021-22 / pg. 723

MINISTÉRIO PÚBLICO
DO ESTADO DA BAHIA

DESPACHO

Em atendimento ao despacho da SGA - ATJ (0196592), juntamos os orçamentos das empresas Stefanini e Ibliss, nos documentos Orçamento 01_Atualizado e Orçamento 02_atualizado, respectivamente. No que se refere a empresa VIVO não conseguimos resposta em tempo, conforme documento E-mails_Enviados_VIVO comprovando nossas solicitações. Entretanto, considerando os documentos (0164289) e (0168072) não vislumbramos alteração no valor da referida proposta.

Assim encaminhamos este expediente para os devidos prosseguimentos.

Documento assinado eletronicamente por **Iaçanã Lima de Jesus Carneiro** em 28/07/2021, às 14:f 2, con.orme artº 1I, "", tLb, da 9ei 11ºf 17/2006º

A autenticidade do documento pode ser con.erida no site https://seiºsistemasºmpLaºmpºLr/sei/controlador_externoºphp?acao=documento_con.erir&id_orgao_acesso_externo=0 in.ormando o código veri.icador **0202844** e o código CRC **93062136º**

Voltar Imprimir

CAIXA ECONÔMICA FEDERAL

Certificado de Regularidade do FGTS - CRF

Inscrição: 24.691.488/0001-09
Razão Social: STEFANINI RAFAEL SEGURANCA E DEFESA SA
Endereço: AV EUSEBIO MATOSO 1375 AND 8 SL 801 E 802 / BUTANTA / SAO PAULO / SP / 05423-905

A Caixa Econômica Federal, no uso da atribuição que lhe confere o Art. 7, da Lei 8.036, de 11 de maio de 1990, certifica que, nesta data, a empresa acima identificada encontra-se em situação regular perante o Fundo de Garantia do Tempo de Servico - FGTS.

O presente Certificado não servirá de prova contra cobrança de quaisquer débitos referentes a contribuições e/ou encargos devidos, decorrentes das obrigações com o FGTS.

Validade: 24/09/2021 a 23/10/2021

Certificação Número: 2021092402135765950613

Informação obtida em 01/10/2021 18:25:10

A utilização deste Certificado para os fins previstos em Lei esta condicionada a verificação de autenticidade no site da Caixa: **www.caixa.gov.br**

Certidão FGTS (0209012) SEI 19.09.02684.0011790/2021-22 / pg. 725

PREFEITURA DE
SÃO PAULO
FAZENDA

SECRETARIA MUNICIPAL DA FAZENDA

Certidão Conjunta de Débitos de Tributos Mobiliários

Certidão Número: 0987306 - 2021

CPF/CNPJ Raiz: 24.691.488/
Contribuinte: STEFANINI RAFAEL SEGURANCA E DEFESA S.A.

Liberação: 16/09/2021
Validade: 15/03/2022

Tributos Abrangidos:
Imposto Sobre Serviços - ISS
Taxa de Fiscalização de Localização Instalação e Funcionamento
Taxa de Fiscalização de Anúncio - TFA
Taxa de Fiscalização de Estabelecimento - TFE
Taxa de Resíduos Sólidos de Serviços de Saúde - TRSS (incidência a partir de Jan/2011)
Imposto Sobre Transmissão de Bens Imóveis - ITBI

Unidades Tributárias:

CCM 5.603.212-9- Inicio atv :17/10/2016 (AV EUSEBIO MATOSO 1375, 1375 - CEP: 05423-905)

Ressalvado o direito de a Fazenda Municipal cobrar e inscrever quaisquer dívidas de responsabilidade do sujeito passivo que vierem a ser apuradas ou que se verifiquem a qualquer tempo, inclusive em relação ao período contido neste documento, relativas a tributos administrados pela Secretaria Municipal da Fazenda e a inscrições em Dívida Ativa Municipal, junto à Procuradoria Geral do Município é certificado que a Situação Fiscal do Contribuinte supra, referente aos créditos tributários inscritos e não inscritos na Dívida Ativa abrangidos por esta certidão, até a presente data é: **REGULAR.**

A aceitação desta certidão está condicionada à verificação de sua autenticidade na Internet, no endereço http://www.prefeitura.sp.gov.br/cidade/secretarias/fazenda/.
Qualquer rasura invalidará este documento.

SITUAÇÃO REGULAR

Certidão expedida com base na Portaria Conjunta SF/PGM nº 4, de 12 de abril de 2017, Instrução Normativa SF/SUREM nº 3, de 6 de abril de 2015, Decreto 50.691, de 29 de junho de 2009, Decreto 51.714, de 13 de agosto de 2010; Portaria SF nº 268, de 11 de outubro de 2019 e Portaria SF nº 182, de 04 de agosto de 2021.

Certidão emitida às 18:27:57 horas do dia 01/10/2021 (hora e data de Brasília).

Código de Autenticidade: 66CFC5FB

A autenticidade desta certidão deverá ser confirmada na página da Secretaria Municipal da Fazenda http://www.prefeitura.sp.gov.br/sf

GOVERNO DO ESTADO DA BAHIA

SECRETARIA DA FAZENDA

Emissão: 05/10/2021 16:39

Certidão Negativa de Débitos Tributários

(Emitida para os efeitos dos arts. 113 e 114 da Lei 3.956 de 11 de dezembro de 1981 - Código Tributário do Estado da Bahia)

Certidão Nº: **20214097145**

RAZÃO SOCIAL	
XXXX

MINISTÉRIO PÚBLICO
DO ESTADO DA BAHIA

PARECER

PROCEDIMENTO SEI Nº. 19.09.02684.0011790/2021-22

INTERESSADA: DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

ASSUNTO: DISPENSA DE LICITAÇÃO

EMENTA: DISPENSA DE LICITAÇÃO. VARREDURA DE VULNERABILIDADES E TESTES DE INTRUSÃO EM APLICAÇÃO *WEB,* NO FORMATO *BLACK-BOX*. CONTRATAÇÃO DIRETA. APLICAÇÃO DO ART. 59, INCISO II, DA LEI ESTADUAL Nº 9.433/2005. PELO DEFERIMENTO. ATO NORMATIVO Nº. 007/2020, COM AS ALTERAÇÕES DOS ATOS NORMATIVOS Nº 048/2020, 035/2021 E 046/2021. NECESSÁRIA MANIFESTAÇÃO PRÉVIA DO COMITÊ DE REPACTUAÇÃO ORÇAMENTÁRIA.

PARECER Nº. 524/2021

Trata-se de autorização para contratação direta, através de **Dispensa de Licitação,** em favor da empresa **Stefanini Rafael Segurança e Defesa S.A.,** no valor total de **R$ 8.202,67** (oito mil duzentos e dois reais e sessenta e sete centavos), visando à **prestação de serviços técnicos, na área de tecnologia da informação, para a varredura de vulnerabilidades e testes de intrusão - PENTEST – em uma aplicação *Web* (Voto Digital), no formato *Black-Box*, nos termos e condições especificados no competente Termo de Referência.**

A despesa correrá por conta do Projeto/Atividade 2002 Manutenção de Serviços de Tecnologia da Informação, Elemento 33.90.40, cujo saldo de dotação é de **R$ 2.149.795,28 (dois milhões cento e quarenta e nove mil setecentos e noventa e cinco reais e vinte e oito centavos).**

Anexados ao procedimento: formulário de autorização de dispensa, termo de referência para o objeto, justificativa para a contratação, pesquisa de mercado, proposta comercial da pessoa jurídica a ser contratada, documentos de representação, minuta de contrato a ser firmado para o objeto e certidões de regularidade fiscal e trabalhista, além de outros documentos relativos à avença.

A unidade responsável, justificando a pretensa contratação, manifestou-se, *in verbis:*

"(...) O Ministério Público do Estado da Bahia (MPBA) encontra-se em plena transformação digital, passando por mudança de cultura e adoção de novos procedimentos que estão sendo alicerçados pela tecnologia da informação. Neste contexto, a Alta Administração da instituição decidiu pela realização das eleições internas através de sistema informatizado de votação denominado VOTO DIGITAL. Originalmente cedido pelo Ministério Público do Estado de São Paulo com o nome VOTO ELETRÔNICO, o sistema foi instalado e configurado no ambiente tecnológico do MPBA e posteriormente adaptado para funcionar de acordo com as regras estabelecidas pelos seus gestores, passando a ser chamado de VOTO DIGITAL. De forma inovadora, será possibilitado que os membros do MPBA possam votar a partir de computadores ou dispositivos móveis conectados à internet, mediante dupla autenticação e outros requisitos de segurança.

É sabido que os processos eleitorais são sujeitos a críticas ainda mais quando envolvem tecnologia da informação e comunicação. Objetivando garantir a máxima segurança da informação possível no sistema VOTO DIGITAL, o MPBA vem realizando ações tecnológicas e procedimentais visando garantir a lisura e transparência de todo o processo eleitoral assim como das ferramentas tecnológicas envolvidas.

O MPBA entende que a realização de um Teste de Intrusão - PENTEST -, conjunto de testes visando detectar falhas e/ou vulnerabilidades da referida aplicação e na infraestrutura que a suporta, utilizando técnicas dos Hackers éticos - especialistas em segurança da informação, irá possibilitar o conhecimento maior sobre a aplicação e sua infra com o intuito de ter um ambiente o mais seguro possível, atendendo aos princípios basilares da segurança da informação - Integridade, Confiabilidade e Disponibilidade.

A presente contratação visa a realização de uma análise independente e externa a área de TI do MPBA com o objetivo de eliminar eventuais vulnerabilidades do sistema VOTO DIGITAL contribuindo para que o mesmo seja executado de maneira segura. (...)"

No caso *sub oculi*, a hipótese é de dispensa, tendo em vista que a situação se amolda ao que dispõe o art. 59, inciso II, da Lei Estadual nº. 9.433/2005:

Art. 59 – É dispensável a licitação:

(...)

II - para outros serviços e compras de valor até 10% (dez por cento) do limite previsto para compras e serviços que não sejam de engenharia, na modalidade de convite, e para alienações, nos casos previstos nesta Lei, desde que não se refiram a parcelas de um mesmo serviço, compra ou alienação de maior vulto que possa ser realizada de uma só vez;

Com efeito, o art. 55 da referida Lei, com as alterações advindas da Lei nº 13.591/2016, determina que, para a definição das modalidades licitatórias serão observados os limites de 100% (cem por cento) do valor fixado para situação idêntica pela União, o que significa que o valor de referência para a hipótese sob comento é de R$ 17.600,00 (dezessete mil e seiscentos reais)[1]. Destarte, verifica-se que o custo estipulado para a almejada contratação se encontra dentro do limite permitido.

Ademais, o critério para a escolha da contratada foi o menor valor oferecido dentre as empresas consultadas, razão pela qual se justifica, de igual modo, o preço obtido.

Por derradeiro, a minuta contratual obedece às disposições da Lei nº. 9.433/2005, em especial as exigências do art. 126 e seguintes, constando as cláusulas referentes ao objeto, regime de execução, entrega, recebimento, dotação orçamentária, preço, acréscimos e supressões, condições de pagamento, retenção dos tributos, reajustamento, revisão de preços, vigência, obrigações dos contratantes, fiscalização, penalidades, rescisão, vinculação ao processo de dispensa de licitação, publicidade, foro e disposições gerais.

Vale destacar, porém, que a Procuradoria-Geral de Justiça, ao editar o Ato Normativo nº 007/2020, alterado pelos Atos Normativos nº 048/2020, 035/2021 e 046/2021, que dispõe sobre medidas de redução, contenção e controle de gastos com custeio e investimento, no âmbito deste Parquet, estabeleceu nos arts. 3º, XIII, e 5º, *in verbis:*

Art. 3º Ficam suspensas as despesas decorrentes das seguintes atividades no âmbito de todo o Ministério Público do Estado da Bahia:

(...)

XIII – Contratos não essenciais;

(...)

Art. 5º A execução de despesa contrária às disposições contidas neste Ato condicionar-se-á à existência de disponibilidade orçamentária, à urgência, ao risco imediato de suspensão dos serviços, e à manifestação prévia do Comitê de Repactuação Orçamentária.

Nada obstante, diante da lacuna referente ao conceito de "contratos essenciais", socorremo-nos às disposições contidas na legislação pátria, em especial a Lei nº 7.783/1989, cujo art. 10[2] define a expressão debatida. Tal definição é replicada no Decreto Federal nº. 10.282/2020, que regulamenta a Lei nº. 13.979/2020.

Com efeito, uma vez que o pretenso objeto não encontra guarida no mencionado rol de serviços essenciais, as despesas correlatas restam, a princípio, suspensas, carecendo de manifestação prévia do Comitê de Repactuação Orçamentária.

Considerando a existência de respaldo legal para a presente hipótese, **esta Assessoria Técnico-Jurídica opina pelo deferimento do pleito, aprovando a minuta de contrato apresentada, sem prejuízo da necessidade de submissão do expediente ao Comitê de Repactuação Orçamentária, nos termos do art. 5º, do Ato Normativo nº. 007/2020, alterado pelos Atos Normativos nº 048/2020, 035/2021 e 046/2021.**

É o parecer, s.m.j.

Salvador, 05 de outubro de 2021.

Belª. Maria Paula Simões Silva
Assessora/SGA
Matrícula 351.869

Bel. Gláucio Matos Santos de Cerqueira
Assistente de Gestão II
Apoio Processual ATJ/SGA
Matrícula 352.748

[1] *Vide art. 2º do Decreto Estadual nº. 18.489/2018.*

[2] *Art. 10 São considerados serviços ou atividades essenciais: I - tratamento e abastecimento de água; produção e distribuição de energia elétrica, gás e combustíveis; II - assistência médica e hospitalar; III - distribuição e comercialização de medicamentos e alimentos; IV - funerários; V - transporte coletivo; VI - captação e tratamento de esgoto e lixo; VII - telecomunicações; VIII - guarda, uso e controle de substâncias radioativas, equipamentos e materiais nucleares; IX - processamento de dados ligados a serviços essenciais; X - controle de tráfego aéreo e navegação aérea; (Redação dada pela Lei nº 13.903, de 2019) XI compensação bancária. XII - atividades médico-periciais relacionadas com o regime geral de previdência social e a assistência social; (Incluído pela Lei nº 13.846, de 2019) XIII - atividades médico-periciais relacionadas com a caracterização do impedimento físico, mental, intelectual ou sensorial da pessoa com*

deficiência, por meio da integração de equipes multiprofissionais e interdisciplinares, para fins de reconhecimento de direitos previstos em lei, em especial na Lei nº 13.146, de 6 de julho de 2015 (Estatuto da Pessoa com Deficiência); e (Incluído pela Lei nº 13.846, de 2019) XIV - outras prestações médico-periciais da carreira de Perito Médico Federal indispensáveis ao atendimento das necessidades inadiáveis da comunidade. (Incluído pela Lei nº 13.846, de 2019) XV - atividades portuárias. (Incluído pela Medida Provisória nº 945, de 2020).

Documento assinado eletronicamente por **Maria Paula Simoes Silva** em 29/02/72701, s 0à:3f 1con.orme artº 0l 1""1bLb1da 4ei 00ºf 06/7229º

Documento assinado eletronicamente por **Glaucio Matos Santos Cerqueira** em 2à/02/72701, s 26:391con.orme artº 0l 1""1bLb1da 4ei 00ºf 06/7229º

A autenticidade do documento pode ser con.erida no site https://seiºsistemasºmpLaºmpºLr/sei/controlador_externoºphp?acao=documento_con.erir&id_orgao_acesso_externo=2 in.ormando o código veri.icador **0209093** e o código CRC **0894486Cº**

MINISTÉRIO PÚBLICO
DO ESTADO DA BAHIA

DESPACHO

Acolho manifestação da Assessoria Técnico-Jurídica pelos fundamentos expostos no Parecer nº 524/2021 e, considerando os arts. 3º e 5º do Ato Normativo nº 007/2020, alterado pelo Atos Normativos nº 048/2020, 035/2021 e 046/2021, com efeito até 31 de dezembro de 2021, encaminhe-se o presente expediente ao Comitê de Repactuação Orçamentária para análise do pleito.

Documento assinado eletronicamente por **Frederico Welington Silveira Soares** em 07/10/2021, às 15:04, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.sistemas.mpba.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0210714** e o código CRC **A9B9E920**.

MINISTÉRIO PÚBLICO
DO ESTADO DA BAHIA

DESPACHO

Encaminhe-se o presente expediente à Chefia de Gabinete informando que, em reunião do Comitê de Repactuação Orçamentária realizada no dia 20/10/2021, foram tratados dentre outros temas, a solicitação formulada pela Diretoria de Tecnologia da Informação, referente à prestação de serviços técnicos, na área de tecnologia da informação, para a varredura de vulnerabilidades e testes de intrusão - PENTEST em uma aplicação Web (Voto Digital), no formato Black-Box e valor global de R$ 8.202,67.

Após explanações, todos os presentes se manifestaram pelo **deferimento** do pleito.

Ante ao exposto, encaminhamos o procedimento juntamente com cópia da ata da referida reunião para deliberação final da Procuradoria Geral de Justiça conforme prevê o Ato Normativo 07/2020, alterado pelos Atos Normativos nº 048/2020, nº 035 de 28 de junho de 2021 e nº 046 de 28 de setembro de 2021, com efeitos extensivos até 31 de dezembro de 2021.

Em tempo, nos colocamos à disposição para os esclarecimentos adicionais que se fizerem necessários.

Cordialmente,

FREDERICO WELINGTON SILVEIRA SOARES
Superintendente de Gestão Administrativa

Documento assinado eletronicamente por **Frederico Welington Silveira Soares** em 02/81/0108, às 8: f82, con.orme artº 8l, "", bLb, da 4ei 88º986/011: º

A autenticidade do documento pode ser con.erida no site httpsf//seiºsistemasºmpLaºmpºLr/sei/controlador_externoºphp?acao=documento_con.erir&id_orgao_acesso_externo=1 in.ormando o código veri.icador **0223243** e o código CRC **6672B14E**º

MINISTÉRIO PÚBLICO
DO ESTADO DA BAHIA

ATA

ATA DE REUNIÃO

COMITÊ DE REPACTUAÇÃO ORÇAMENTÁRIA

Aos vinte dias do mês de outubro do corrente ano, às dez horas, se reuniram por meio de videoconferência, a Corregedora Geral, Dra. Cleonice de Souza Lima, o Secretário Geral Adjunto, Dr. Ricardo de Assis Andrade e o Superintendente de Gestão Administrativa, Frederico Welington Silveira Soares, membros do Comitê de Repactuação Orçamentária.

Foram devidamente justificadas as ausências do Chefe de Gabinete, Dr. Pedro Maia, da representante do Colégio de Procuradores de Justiça, Dra. Elza Maria de Souza e do Coordenador da Gestão Estratégica, Dr. Lourival Miranda de Almeida Júnior.

O Superintendente cumprimentou a todos os presentes, bem como informou que estão devidamente justificadas as ausências de Dr. Pedro Maia, Dra. Elza e Dr. Lourival. O Superintendente informou ainda que não foi possível a realização da reunião na semana passada, em função do feriado, além da realização da manifestação contra a PEC nº. 05/2021 e incompatibilidade de agendas. O Superintendente pontuou que iniciará a avaliação dos itens contidos na pauta, relativos aos Processos de Dispensa de Licitação, cujo primeiro item, Processo Eletrônico SEI Nº. 19.09.02684.0011790/2021-22, oriundo da Diretoria de Tecnologia da Informação, se refere a prestação de serviços técnicos, na área de tecnologia da informação, para a varredura de vulnerabilidades e testes de intrusão - PENTEST – em uma aplicação Web (Voto Digital), no formato Black-Box e valor global de R$ 8.202,67. Explicou o Superintendente como será realizado o serviço, relativa a presente contratação, bem como acrescentou que serão realizadas duas eleições importantes, através do voto digital, no ano vindouro. A eleição para o Conselho Superior do Ministério Público e posteriormente, a eleição para Procurador-Geral de Justiça, reforçando a importância da contratação em questão. Abriu para discussão o Superintendente, iniciando por Dra. Cleonice. Dra. Cleonice fez alguns questionamentos ao Superintendente, relativos à contratação, que foram devidamente esclarecidos. Após os esclarecimentos fornecidos pelo Superintendente, Dra. Cleonice fez a sua explanação, votando pela aprovação. Dr. Ricardo e o Superintendente acompanharam o voto de Dra. Cleonice.

O Superintendente sugeriu a aprovação em bloco do segundo ao quarto item da pauta, bem como relatou que os processos possuem objetos similares e que estão devidamente instruídos.

O segundo item da pauta, Processo Eletrônico SEI Nº. 19.09.01079.0011863/2021-79, oriundo da Promotoria de Justiça Regional de Paulo Afonso, se refere a prestação de serviços de instalação de condicionadores de ar split e manutenção preventiva em condicionadores de ar instalados na Promotoria de Justiça Regional.de Paulo Afonso, no valor de R$ 2.240,00.

O terceiro item da pauta, Processo Eletrônico SEI Nº. 19.09.00925.0015454/2021-33, oriundo da Promotoria de Justiça Regional de Barreiras, se refere a prestação de serviços de limpeza interna e externa em condicionadores de ar da Promotoria de Justiça Regional de Barreiras, Comitê Interinstitucional de Recuperação de Ativos - CIRA e Promotoria de Justiça de Luís Eduardo Magalhães, no valor de R$ 5.990,00.

O quarto item da pauta, Processo Eletrônico SEI Nº. 19.09.00896.0017441/2021-66, oriundo da Promotoria de Justiça Regional de Ilhéus, se refere a prestação de serviços de manutenção preventiva, recarga de gás e instalação de ar-condicionado na Promotoria de Justiça Regional de Ilhéus, no valor de R$ 4.900,00.

Abriu para discussão o Superintendente, iniciando por Dra. Cleonice. Dra. Cleonice fez a sua explanação, votando pela aprovação em bloco do segundo ao quarto item da pauta. Dr. Ricardo e o Superintendente acompanharam o voto de Dra. Cleonice.

O quinto item da pauta, Processo Eletrônico SEI Nº. 19.09.01010.0015538/2021-57, oriundo da Promotoria de Justiça Regional de Itaberaba, se refere a prestação de serviços de fornecimento de 180 garrafões de água mineral natural, sem gás, com capacidade para 20 litros, no valor de R$ 1.620,00/ano. Esclareceu o Superintendente que cada garrafão de água, representa o valor unitário de R$ 9,00 e que a Coordenadora de Itaberaba, Dra. Marisa Jansen, justifica que ainda não foi instalado o purificador de água, uma vez que possui muitos pombos nas proximidades do reservatório de água da promotoria e que na última limpeza realizada foi detectado algumas situações. Ressaltou o Superintendente que serão instalados os purificadores de água, tão logo seja efetuado o retorno na sua totalidade, nas promotorias que tenham possibilidade de instalação. Abriu para discussão o Superintendente, iniciando por Dra. Cleonice. Dra. Cleonice fez a sua explanação, votando pela aprovação. Dr. Ricardo e o Superintendente acompanharam o voto de Dra. Cleonice.

O sexto item da pauta, Processo Eletrônico SEI Nº. 19.09.00878.0016106/2021-60, oriundo da Promotoria de Justiça Regional de Vitória da Conquista, se refere a prestação de serviços de jardinagem e manutenção em toda a área verde da Promotoria de Justiça Regional de Vitória da Conquista, no valor de R$ 2.760,00/ano.

O sétimo item da pauta, Processo Eletrônico SEI Nº. 19.09.00925.0015663/2021-41, oriundo da Promotoria de Justiça Regional de Barreiras, se refere a prestação de serviços de jardinagem, com a finalidade de realizar a manutenção da área verde da Promotoria de Justiça Regional de Barreiras, no valor de R$ 6.000,00/ano.

Após as explicações efetuadas, o Superintendente sugeriu a avaliação em bloco do quinto e sexto item da pauta. Abriu para discussão o Superintendente, iniciando por Dra. Cleonice. Dra. Cleonice fez a sua explanação, votando pela aprovação em bloco do quinto e sexto item da pauta. Dr. Ricardo e o Superintendente acompanharam o voto de Dra. Cleonice.

O oitavo item da pauta, Processo Eletrônico SEI Nº. 19.09.01043.0015960/2021-03, oriundo da Promotoria de Justiça Regional de Jacobina, se refere a prestação de serviços de pintura com fornecimento de material, interna, com tinta acrílica, cor branco neve, em parede e forro, incluindo tratamento de trechos

danificados por infiltração para Promotoria de Justiça Regional de Jacobina, no valor de R$ 4.331,60. Abriu para discussão o Superintendente, iniciando por Dra. Cleonice. Dra. Cleonice perguntou ao Superintendente se o fornecimento do material e a mão de obra será efetuada localmente. O Superintendente constatou no processo que tanto o serviço quanto o material serão fornecidos localmente. Dra. Cleonice fez a sua explanação, votando pela aprovação. Dr. Ricardo e o Superintendente acompanharam o voto de Dra. Cleonice.

O nono item da pauta, Processo Eletrônico SEI Nº. 19.09.00878.0008148/2021-32, oriundo da Promotoria de Justiça Regional de Vitória da Conquista, se refere a prestação de serviços de substituição do setor danificado, reparo, manutenção e substituição das placas de policarbonato na estrutura metálica da cobertura da entrada principal da Promotoria de Justiça Regional de Vitória da Conquista, no valor de R$ 15.899,94. Esclareceu o Superintendente que o processo está devidamente instruído. Dr. Ricardo fez um questionamento ao Superintendente que foi devidamente esclarecido. Abriu para discussão o Superintendente, iniciando por Dra. Cleonice. Dra. Cleonice fez a sua explanação, bem como sugeriu e aprovou em bloco o nono e o décimo item da pauta. Dr. Ricardo e o Superintendente acompanharam o voto de Dra. Cleonice.

O décimo item da pauta, Processo Eletrônico SEI Nº. 19.09.01148.0016810/2021-24, oriundo da Promotoria de Justiça Regional de Teixeira de Freitas, se refere a prestação de serviços de recarga de 07 extintores de incêndio para Promotoria de Justiça Regional de Teixeira de Freitas, no valor de R$ 295,00.

O décimo primeiro item da pauta, Processo Eletrônico SEI Nº. 19.09.00857.0014161/2021-08, oriundo da Diretoria Administrativa, se refere a prestação de serviços de seguro contra incêndio, queda de raio, explosão de qualquer natureza, danos elétricos e demais coberturas adicionais para o imóvel de propriedade do Ministério Público situado no CAB, no valor de R$ 10.047,30/ano. Esclareceu o Superintendente que a Instituição possui um contrato vigente (Contrato nº. 142/2016-SGA), referente ao mesmo objeto, que irá vencer em 09 de novembro de 2021, possuindo o valor de R$ 10.800,00 e que a presente contratação, representará uma redução do valor contratado, passando de R$ 10.800,00 para R$ 10.047,30. Ressaltou o Superintendente que o Comitê aprovou, no dia 07 de julho de 2021, a contratação do seguro por procedimento licitatório, estimado em R$ 15.446,33. Ressaltou ainda o Superintendente que devido ao grande volume de licitações em andamento, priorizadas pelo Gabinete, deliberou-se pela contratação do mencionado serviço, através de dispensa de licitação, seguindo todas as recomendações, do ponto de vista jurídico, destacando a redução do valor do contrato atual, bem como o valor estimado para realização da licitação. Abriu para discussão o Superintendente, iniciando por Dra. Cleonice. Dra. Cleonice fez a sua explanação, votando pela aprovação. Dr. Ricardo e o Superintendente acompanharam o voto de Dra. Cleonice.

O décimo segundo item da pauta, Processo Eletrônico SEI Nº. 19.09.01355.0016010/2021-79, oriundo da Promotoria de Justiça de Ribeira do Pombal, se refere a prestação de serviços de mensageiro motorizado, no valor de R$ 7.200,00/ano. Esclareceu o Superintendente que foi celebrado contrato anterior no valor de R$ 6.120,00 e que a presente solicitação se refere a uma nova contratação no valor de R$ 7.200,00 por 01 ano. Abriu para discussão o Superintendente, iniciando por Dra. Cleonice. Dra. Cleonice fez a sua explanação, votando pela aprovação. Dr. Ricardo e o Superintendente acompanharam o voto de Dra. Cleonice.

O décimo terceiro item da pauta, Processo Eletrônico SEI Nº. 19.09.02349.0013896/2021-86, oriundo da Diretoria Administrativa/Coordenação de Serviços Gerais, se refere a prestação de serviços de conserto de 06 fragmentadoras de várias unidades do MPBA, no valor de R$ 2.490,00. Esclareceu o Superintendente que no ano passado, o Comitê aprovou a manutenção de 11 fragmentadoras e que as fragmentadoras, objeto da presente solicitação, referem-se a outros equipamentos e que o valor está compatível com o valor executado para reparo das 11 fragmentadoras. Acrescentou o Superintendente que a justificativa para realização do reparo/manutenção desses equipamentos é mais vantajosa em detrimento da aquisição de um equipamento novo, pois em média o conserto representa o valor de R$ 400,00 e a aquisição de um equipamento novo, representa cerca de R$ 1.900,00. Abriu para discussão o Superintendente, iniciando por Dra. Cleonice. Dra. Cleonice fez a sua explanação, votando pela aprovação. Dr. Ricardo e o Superintendente acompanharam o voto de Dra. Cleonice.

O décimo quarto item da pauta, Processo Eletrônico SEI Nº. 19.09.02345.0016166/2021-74, oriundo da Diretoria de Contratos, Convênios e Licitações/Coordenação de Suprimentos, se refere a aquisição de kit de substituição de cabeça de impressão para duas impressoras, modelo HP DesignJet série T120, localizadas no CIGEO e na CGE, no valor de R$ 3.790,00. Esclareceu o Superintendente que a presente solicitação se refere a aquisição de peça para as impressoras do CIGEO e da CGE, equipamentos específicos dessas unidades, que essas peças serão substituídas e que o procedimento está devidamente instruído com todas as certidões, bem como com o parecer jurídico da Assessoria Técnico-Jurídica da Superintendência. Abriu para discussão o Superintendente, iniciando por Dra. Cleonice. Dra. Cleonice fez a sua explanação, votando pela aprovação. Dr. Ricardo e o Superintendente acompanharam o voto de Dra. Cleonice.

O décimo quinto item da pauta, Processo Eletrônico SEI Nº. 19.09.45340.0015388/2021-24, oriundo do CEAF, se refere a prestação de serviços de seleção pública de estudantes de graduação e de pós-graduação, da área de Direito, com a aplicação das provas integralmente na modalidade on-line, no valor de R$ 77.000,00. Esclareceu o Superintendente que a arrecadação com a inscrição, realizada em todo concurso, servirá para custear as despesas com a execução do próprio concurso. Dr. Ricardo fez uma pergunta ao Superintendente com relação a aprovação da despesa em outra ocasião. Dra. Cleonice acrescentou algumas informações e o Superintendente pontuou que a presente contratação se refere a seleção de estagiários de Direito de graduação e pós-graduação. Esclareceu ainda o Superintendente que o processo é extenso, que foi realizada pesquisa de mercado com as empresas especializadas em seleções públicas e que o Instituto AOCP apresentou o menor preço dentre as empresas que responderam à solicitação de proposta. Salientou o Superintendente que a aprovação efetuada em outra ocasião foi para seleção de estagiários de direito para atendimento das Promotorias de Justiça do Interior e será realizada pela Fundação Getúlio Vargas. Salientou ainda o Superintendente que a presente contratação se refere a seleção de estagiários de direito de graduação e pós-graduação para atendimento das Promotorias da Capital e será realizada pelo Instituto AOCP, pois a Cesgranrio, a Fundação Carlos Chaga e a Fundação Getúlio Vargas manifestaram que não poderão assumir o compromisso. Acrescentou o Superintendente que o processo está devidamente instruído. Abriu para discussão o Superintendente, iniciando por Dra. Cleonice. Dra. Cleonice fez a sua explanação, votando pela aprovação. Dr. Ricardo e o Superintendente acompanharam o voto de Dra. Cleonice.

Encerrada a avaliação dos processos de Dispensa de Licitação, o Superintendente passou a tratar dos processos referentes a Inexigibilidade de Licitação.

O décimo sexto item da pauta, Processo Eletrônico SEI Nº. 19.09.45340.0016517/2021-70, oriundo do CEAF, se refere a aquisição de assinatura anual da Biblioteca Digital Proview, com até 100 acessos simultâneos, no valor de R$ 36.186,72/ano. Esclareceu o Superintendente que Dr. Tiago justifica que o acesso à Biblioteca ProView complementa as ações do CEAF, permitindo o enriquecimento do acervo da Biblioteca, como também possibilita o acesso de todos os colaboradores da instituição, tanto no interior quanto na Capital, no exercício de suas atividades, com agilidade e eficácia, além de fortalecer os programas institucionais e projetos de valorização técnica e acadêmica com menor custo por usuário. Esclareceu Dr. Tiago justifica ainda que a Plataforma da Editora Revista dos Tribunais possui obras de autores renomados de diversos assuntos jurídicos e, principalmente, assuntos atrelados às áreas de atuação do MPBA. O conteúdo multidisciplinar que a compõe vai ao encontro da missão institucional do Ministério Público, vez que, por perpassar disciplinas insertas nos ramos do Direito Público e Privado, empodera, sem sombra de dúvidas, sua atuação, como órgão agente e interveniente, na defesa da ordem jurídica, do regime democrático e dos interesses sociais e individuais indisponíveis. Quanto ao preço apresentado para o Ministério Público do Estado da Bahia, mostra-se compatível ou abaixo do praticado para outras Instituições governamentais, conforme verificação das notas fiscais da Justiça Federal do Rio Grande do Sul, no valor de R$ 44.388,08, do Tribunal de Contas do Estado do Tocantins, no valor de R$ 41.205,12 e do Tribunal Regional Eleitoral do Paraná, no valor de R$ 37.777,00. Abriu para discussão o Superintendente, iniciando por Dra. Cleonice. Dra. Cleonice fez a sua explanação, votando pela aprovação. Dr. Ricardo e o Superintendente acompanharam o voto de Dra. Cleonice.

O décimo sétimo item da pauta, Processo Eletrônico SEI Nº. 19.09.45340.0016897/2021-14, oriundo do CEAF, se refere a inscrição da servidora Fabíola Barbosa da Silva Souza, lotada na Biblioteca, no Curso Conteúdo Digital para Bibliotecas, na modalidade online, com carga horária de 20h, no valor de R$ 366,45. Esclareceu o Superintendente que Dr. Tiago justifica que o curso visa o aprimoramento profissional diante da necessidade de atuar no Sistema de Bibliotecas, incluindo recursos digitais e que abordará os principais aspectos relacionados a inclusão de livros digitais em coleções de bibliotecas, desde obras gratuitas até o conteúdo licenciado e noções gerais de direitos autorais, licenciamento e gestão de conteúdo digital. Esclareceu ainda o Superintendente que Dr. Tiago justifica ainda que, diante da necessidade de gerenciamento eficiente das Bibliotecas Digitais existentes atualmente na Instituição, como a "Biblioteca Digital ProView", da Editora Revista dos Tribunais, faz-se necessária a capacitação profissional da referida servidora. Abriu para discussão o Superintendente, iniciando por Dra. Cleonice. Dra. Cleonice fez a sua explanação, votando pela aprovação. Dr. Ricardo e o Superintendente acompanharam o voto de Dra. Cleonice.

O décimo oitavo item da pauta, Processo Eletrônico SEI Nº. 19.09.00856.0017583/2021-53, oriundo da Diretoria Administrativa, se refere a inscrição dos servidores Ana Gabriela Reis Nogueira e Leonardo Borges Castellar Sampaio, lotados na Coordenação de Transportes, no Curso de Gestão Profissional de Frotas Públicas, na modalidade online, com carga horária de 12h, no valor de R$ 2.514,00. Contextualizou o Superintendente que foi realizada uma alteração na gerência da Coordenação de Transportes e que os atuais responsáveis verificaram a possibilidade de participação no mencionado curso, visando a melhoria daquela Coordenação, bem como eficiência e economia da frota da Instituição. Acrescentou o Superintendente que o curso de capacitação possui o valor de R$ 2.514,00 para os 02 servidores, Ana Gabriela e Leonardo Castellar, que está de acordo com o orçamento da Diretoria Administrativa para capacitação. Acrescentou ainda o Superintendente que o edital está em tramite para realização de aluguel de frotas, pois demonstra que é mais econômico com relação a aquisição de veículos para Instituição. O Superintendente antecipou o seu voto pela aprovação, bem como iniciou a discussão por Dra. Cleonice. Dra. Cleonice fez a sua explanação, votando pela aprovação, com a recomendação que seja realizada uma capacitação para os motoristas da Instituição. Dr. Ricardo acompanhou o voto de Dra. Cleonice, bem como o voto de Superintendente.

Encerrada a avaliação dos processos de Inexigibilidade de Licitação, o Superintendente passou a tratar dos processos referentes a Licitação.

O décimo nono item da pauta, Processo Eletrônico SEI Nº. 19.09.02349.0016184/2021-97, oriundo da Diretoria Administrativa/Coordenação de Serviços Gerais, se refere a prestação de serviços de manutenção corretiva em mobiliários em madeira e em aço, no valor de R$ 77.402,33. Esclareceu o Superintendente que o pleito em questão se refere a manutenção corretiva nos mobiliários da Instituição (cadeiras, poltronas, mesas, armários, dentre outros) e que essa prática já existe há um tempo na Instituição, visando a realização de reparo em mobiliários em madeira e em aço, exemplificando que não justifica a aquisição de uma cadeira giratória com braço nova, em razão de apresentar apenas o braço quebrado. O Superintendente compartilhou a sua tela, apresentando aos membros o processo, motivo da avaliação, bem como pontuou que a Diretoria Administrativa fez uma estimativa, baseado em aproximadamente 280 itens para realização do reparo/manutenção nos mobiliários, sendo desnecessária uma nova aquisição. Esclareceu o Superintendente que o pagamento dessa despesa será realizado, de acordo com a sua utilização. Acrescentou o Superintendente que o valor estimado de R$ 77.402,33 para realização da licitação, quando ocorrer o certame, a tendência é que o valor reduza. Ressaltou o Superintendente que a presente contratação é muito válida, conforme sua execução ao longo dos anos. Abriu para discussão o Superintendente, iniciando por Dra. Cleonice. Dra. Cleonice fez a sua explanação, votando pela aprovação. Dr. Ricardo e o Superintendente acompanharam o voto de Dra. Cleonice.

O vigésimo item da pauta, Processo Eletrônico SEI Nº. 19.09.02004.0007174/2020-61, oriundo da CECOM/Assessoria de Imprensa, se refere a prestação de serviços de monitoramento de notícias e clipagem jornalística de mídias de rádio, tv, jornais, sites, blogs e portais, no valor de R$ 170.000,00. Esclareceu o Superintendente que a presente licitação foi aprovada pelo Comitê na reunião realizada no dia 26 de outubro de 2021, porém a licitação foi impugnada e o processo retornou para nova apreciação do Comitê, em razão da necessidade de ajustes na lógica dos serviços, bem como a atualização do valor estimado, passando de R$ 150.800,00 para R$ 170.000,00. Abriu para discussão o Superintendente, iniciando por Dra. Cleonice. Dra. Cleonice fez a sua explanação, votando pela aprovação. Dr. Ricardo e o Superintendente acompanharam o voto de Dra. Cleonice.

O vigésimo primeiro item da pauta, Processo Eletrônico SEI Nº. 19.09.02336.0015688/2021-88, oriundo da Diretoria de Engenharia e Arquitetura/Coordenação de Manutenção Predial, se refere a aquisição de Lâmpadas LED, no valor de R$ 26.428,50. Esclareceu o Superintendente que a presente licitação atenderá as Unidades da Capital e do Interior e que serão adquiridas lâmpadas de diferentes tipos.

Prosseguindo com a reunião, o Superintendente na sequência pontuou que o vigésimo segundo item da pauta, Processo Eletrônico SEI Nº. 19.09.02349.0017165/2021-77, oriundo da Diretoria Administrativa/Coordenação de Serviços Gerais, se refere a prestação de serviços de desinsetização, desratização, descupinização e fumacê a serem executados nas dependências dos prédios do Ministério Público do Estado da Bahia, localizados em Salvador, no valor de R$ 149.813,40. Esclareceu o Superintendente que a presente prestação de serviços será realizada na Sede CAB, Nazaré, CEAF e Palacete Ferraro e que o valor estimado para realização do mencionado serviço é de R$ 149.813,40, com pelo menos 04 serviços dessa natureza em cada prédio. Esclareceu ainda o Superintendente que o serviço será realizado por 01 ano. Abriu para discussão o Superintendente, iniciando por Dra. Cleonice. Dra. Cleonice fez a sua explanação, votando pela aprovação em bloco do vigésimo primeiro e vigésimo segundo item da pauta. Dr. Ricardo acompanhou o voto de Dra. Cleonice, bem como recomendou que, assim que for possível, a Superintendência avalie a necessidade de aquisição de equipamentos com tecnologia do tipo “inverter”. O Superintendente acompanhou o voto de Dra. Cleonice.

Encerrada a avaliação dos processos de Licitação, o Superintendente passou a tratar dos processos referentes a Sessão Outros.

O vigésimo terceiro item da pauta, Processo Eletrônico SEI Nº. 19.09.00973.0017052/2021-89, oriundo da Promotoria de Justiça Regional de Eunápolis, se refere a solicitação de posto de serviço de vigilância armada 24 horas, no valor de R$ 117.526,20/ano. Esclareceu o Superintendente que a Promotoria de Justiça Regional de Eunápolis possui um posto de serviço de vigilância armada por 12 horas diurno, bem como câmeras de segurança. Esclareceu ainda o Superintendente que foi efetuado contato com a Gerente Administrativa da Regional e que a referida servidora informou que a necessidade da contratação se deve ao fato de eventualmente um promotor ou outro permanecer na Promotoria até às 19h ou 20h. Acrescentou o Superintendente que a pleito em questão foge dos padrões e que já foram negadas outras solicitações nesse mesmo sentido. O Superintendente acrescentou mais algumas informações, contribuindo para avaliação do pleito em questão. Abriu para discussão o Superintendente, iniciando por Dra. Cleonice. Dra. Cleonice fez a sua explanação, votando pelo indeferimento. Dr. Ricardo também fez a sua explanação, votando pelo indeferimento. O Superintendente acompanhou o voto de Dra. Cleonice e Dr. Ricardo.

O Superintendente informou que os próximos processos, do vigésimo quarto ao vigésimo sexto item da pauta, possuem objetos similares, sugerindo a avaliação em bloco.

O Superintendente informou ainda que as Unidades possuem saldo contingenciado, bem como foi avaliado que há condições de atendimento das demandas contidas no vigésimo quarto, vigésimo quinto e vigésimo sexto item da pauta.

O vigésimo quarto item da pauta, Processo Eletrônico SEI Nº. 19.09.02023.0015987/2021-80, oriundo do CEAT, se refere a solicitação de disponibilização de recurso, no valor de R$ 15.000,00. Esclareceu o Superintendente que a solicitação de disponibilização de recurso do CEAT, se refere ao atendimento com diárias e passagens para os Analistas da mencionada unidade.

O vigésimo quinto item da pauta, Processo Eletrônico SEI Nº. 19.09.45340.0017513/2021-58, oriundo do CEAF, se refere a solicitação de liberação de cota orçamentária e de recursos para o evento "Semana do Ministério Público 2021", no valor de R$ 15.000,00.

O vigésimo sexto item da pauta, Processo Eletrônico SEI Nº. 19.09.02259.0017363/2021-46, oriundo do CEAMA/NUMA, se refere a solicitação de descontingenciamento de recurso, no valor de R$ 20.000,00. Esclareceu o Superintendente que consta no oficio de Dr. Yuri Lopes de Mello, que a solicitação de descontingenciamento do recurso, se deve a necessidade de pagamento de despesas com diárias administrativas necessárias à execução de diligências, perícias e ações de fiscalização realizadas pelos servidores, motoristas e policiais lotados nas Promotorias de Justiça Regionais Ambientais, a fim de se verificar a ocorrência de ilícitos ambientais diversos contra a fauna e a flora brasileira objeto de denúncias e inquéritos. Esclareceu ainda o Superintendente que consta o valor de R$ 20.000,00 e que o mesmo está distribuído da seguinte forma: R$ 10.000,00 para despesas com pagamento de diárias para servidores e motoristas e R$ 10.000,00 para despesas com pagamento de diárias para policiais. Dr. Ricardo informou que o Comitê tem deliberado sobre os pedidos de diárias das Ambientais separadamente, citando os pedidos de Dr. Augusto, da Ambiental de Lençóis, bem como de Dr. Julimar, da Ambiental de Santo Antônio de Jesus e a presente solicitação se refere a deliberação de recurso para mesma despesa. O Superintendente pontuou que checará com Dr. Yuri, posteriormente, se a presente solicitação se refere ao recurso necessário para pagamento das diárias solicitadas pelos Promotores de Justiça das Ambientais de Lençóis e Santo Antônio de Jesus. Dra. Cleonice sugeriu adiar a avaliação do presente procedimento para próxima reunião, após o contato que será realizado com Dr. Yuri. Dr. Ricardo registrou que não é contra a liberação do recurso, apenas sanar a dúvida. O Superintendente ratificou que efetuará contato com Dr. Yuri e que o processo será sobrestado para avaliação na próxima reunião.

Após as discussões em torno do tema, Dra. Cleonice, Dr. Ricardo e o Superintendente aprovaram o vigésimo quarto e o vigésimo quinto item da pauta, porém sobrestarão o vigésimo sexto item da pauta para realização de consulta ao Coordenador do CEAMA, Dr. Yuri Lopes de Mello e retorno para apreciação na próxima reunião do Comitê.

O vigésimo sétimo item da pauta, Processo Eletrônico SEI Nº. 19.09.00925.0017327/2021-49, se refere a solicitação de autorização de viagem para realização de reparo no telhado da Sede da Promotoria de Justiça Regional de Barreiras, prevista para o período de 25 a 29 de outubro de 2021, cujo custo estimado é de aproximadamente R$ 6.802,50, levantado pelas Diretorias de Engenharia e Arquitetura e Administrativa contemplando materiais, diárias de servidores, adiantamento, mão-de-obra terceirizada e combustível. Esclareceu o Superintendente que foi discutido com a Regional de Barreiras uma reforma ampla, de proporção maior, orçado em R$ 400.00,00 e a referida regional preferiu que essa intervenção não seja realizada no ano em curso, porém solicitou que fosse realizada algumas intervenções pontuais, em função do período chuvoso em novembro. Esclareceu ainda o Superintendente que o valor apresentado de R$ 6.802,50 está compatível para realização da intervenção pontual, a fim de minimizar algum tipo de dano, ocasionado pelo período chuvoso que se aproxima. Abriu para discussão o Superintendente, iniciando por Dra. Cleonice. Dra. Cleonice fez a sua explanação, votando pela aprovação. Dr. Ricardo e o Superintendente acompanharam o voto de Dra. Cleonice.

O Superintendente avisou que o vigésimo oitavo item da pauta, Processo Eletrônico SEI Nº. 19.09.02156.0015587/2021-39, oriundo da CSI, relativo à solicitação de Dr. Gilberto Costa Amorim Júnior será retirado da pauta, em razão de contato realizado com Dr. Gilberto para um melhor entendimento. Esclareceu o Superintendente que Dr. Gilberto solicitou correção quanto ao entendimento do pleito avaliado na reunião anterior e que não tem possibilidade de cumprir em 83% das situações, o prazo de 10 dias de antecedência, previsto no Ato de Diárias, mas que é possível solicitar com 06, 05 ou 04 dias de antecedência e que a sua solicitação se deve unicamente a prioridade no pagamento. Informou o Superintendente que a solicitação com antecedência de 10 dias é uma regra geral, mas que foi comunicado a Dr. Gilberto que não há problema algum, para os casos de emergência, solicitar a diária com 01 dia de antecedência, apenas corre o risco de não receber o recurso antecipado. Explicou ainda o Superintendente que Dr. Gilberto não se opõe a necessidade de envio de e-mail para a Procuradora-Geral de Justiça, caso seja necessário o registro após a viagem e que os pedidos da CSI são efetuados antes da viagem acontecer. Finalizou o Superintendente, informando que restou esclarecida a solicitação de Dr. Gilberto e que foi pontuado para o mesmo que será realizado um alinhamento com área técnica para verificar o que é possível fazer com relação ao pagamento, em razão de tratar-se de uma unidade sensível e até quantos dias serão necessários para que o pedido seja realizado com antecedência.

Encerrada a avaliação dos processos da Sessão Outros, o Superintendente passou a tratar dos processos referentes as Diárias.

Prosseguindo com a reunião, o Superintendente sugeriu a avaliação em bloco dos processos de diárias, mas salientou que tem ponto de atenção no trigésimo oitavo, trigésimo nono e quadragésimo segundo item da pauta e que, após a leitura e análise, a aprovação será efetuada em bloco e constará o registro no final.

O vigésimo nono item da pauta, Processo SIMP 003.0.2106/2021, se refere a solicitação de meia diária para Dr. Marco Aurélio Rubick da Silva, Titular de Caculé, face a realização de substituição na Promotoria de Justiça de Tanque Novo, no dia 19 de julho de 2021.

O trigésimo item da pauta, Processo Eletrônico SEI Nº. 19.09.00855.0017229/2021-50, se refere a solicitação de 02 meias diárias para Dr. Thiago Cerqueira Fonseca, Titular de Santo Antônio de Jesus, face a realização de substituição na Comarca de Mutuípe, nos dias 19 e 26 de outubro de 2021.

O trigésimo primeiro item da pauta, Processo Eletrônico SEI Nº. 19.09.00855.0017226/2021-29, se refere a solicitação de 03 meias diárias para o motorista Osvaldo Pereira dos Santos, bem como o Policial Militar Leandro Souza dos Anjos, ambos lotados na Base Ambiental de Valença, face a necessidade de deslocamento nos dias 06, 20 e 21 de outubro de 2021, respectivamente, para o município de Jaguaripe/BA, povoado de Cova da Onça (Boipeba, Cairu/BA), e povoado de Garapuá (Morro de São Paulo, Cairu/BA), com a finalidade de cumprimento de mandados de diligência expedidos pelo Promotor de Justiça Dr. Gustavo Fonseca Vieira, em instrução de procedimentos extrajudiciais.

O trigésimo segundo item da pauta, Processo Eletrônico SEI Nº. 19.09.01970.0017209/2021-32, se refere a solicitação de 02 diárias para Dra. Semiana Silva de Oliveira Cardoso, Titular de Feira de Santana, bem como passagens aéreas, face a sua indicação pela Procuradora-Geral de Justiça para participar da 15ª Sessão Ordinária do Plenário do Conselho Nacional do Ministério Público, na qual se deliberará, dentre outros, sobre a proposta de Resolução que dispõe “sobre a Política Institucional de Proteção Integral e de Promoção de Direitos e Apoio às Vítimas de infrações penais e atos infracionais, voltada à assistência, reparação e respeito à dignidade e aos direitos fundamentais”, a partir das 14h do dia 18 de outubro de 2021, em Brasília/DF.

O trigésimo terceiro item da pauta, Processo Eletrônico SEI Nº. 19.09.01998.0016462/2021-96, se refere a solicitação de 02 diárias e meia (risco e vulnerabilidade) para os Policiais Militares, Fredson Ferreira da Cruz, Luciano Muniz de Oliveira e Adilson Vieira dos Santos, lotados na Assistência Militar para acompanhamento da Procuradora-Geral de Justiça, no período de 20 a 22 de outubro de 2021, a Cidade de Vitória da Conquista. O Superintendente informou que a presente solicitação, em razão de outra viagem de Dra. Norma, talvez não esteja mantida, mas está pré-aprovada e caso seja adiada, a referida solicitação também está pré-aprovada para acompanhamento de Dra. Norma.

O trigésimo quarto item da pauta, Processo Eletrônico SEI Nº. 19.09.00855.0017367/2021-46, se refere a solicitação de meia diária (e-Dia 596.7.313/2021) para o motorista Eduardo Santana Freitas, lotado em Feira de Santana, tendo em vista a necessidade de deslocamento para Salvador, no dia 08 de outubro de 2021,

com a finalidade de entrega e retirada de materiais no GAESF e Sede CAB.

O trigésimo quinto item da pauta, Processo Eletrônico SEI Nº. 19.09.00938.0017476/2021-54, se refere a solicitação de 02 meias diárias para o motorista Fernando César Moleiro Lima, lotado em Bom Jesus da Lapa, face a condução de Dr. Marcelo dos Santos C. Porto de Bom Jesus da Lapa para audiência na Comarca de Riacho de Santana, nos dias 26 de agosto e 02 de setembro de 2021.

O trigésimo sexto item da pauta, Processo Eletrônico SEI Nº. 19.09.00855.0017504/2021-35, se refere a solicitação de concessão de diárias para o motorista Ricardo Passos Lima e o Policial Militar Genildo de Souza Pinheiro para os meses de novembro e dezembro de 2021 (dentro do limite máximo permitido por mês), a fim de cumprirem diligências da Promotoria de Justiça Regional Ambiental de Teixeira de Freitas.

O trigésimo sétimo item da pauta, Processo Eletrônico SEI Nº. 19.09.00855.0017503/2021-28, se refere a solicitação de meia diária para Dr. Leandro Mansine Meira Cardoso de Castro, Titular de Guanambi, face a realização de substituição na Comarca de Urandi, no dia 13 de outubro de 2021, bem como meia diária para servidora Elis Titonelli Ferreira Donato, lotada em Guanambi, em razão de acompanhamento de Dr. Leandro Mansine Castro, no exercício de substituição na Comarca de Urandi, no dia 13 de outubro de 2021.

O trigésimo oitavo item da pauta, Processo Eletrônico SEI Nº. 19.09.01690.0018092/2021-37, se refere a solicitação de 02 diárias para Dr. Ariel José Guimarães, Titular de Paripiranga, face a realização de substituição na Comarca de Cícero Dantas, de 26 a 28 de outubro de 2021, bem como 02 diárias para o seu Assessor José Alisson Sousa dos Santos, lotado em Paripiranga, em razão de acompanhamento de Dr. Ariel José Guimarães, no exercício de substituição na Comarca de Cícero Dantas, de 26 a 28 de outubro de 2021. Esclareceu o Superintendente que a Promotoria de Justiça de Cícero Dantas possui 01 servidor lotado. Após discussão em torno da presente solicitação, Dra. Cleonice, Dr. Ricardo e o Superintendente votaram pela aprovação das diárias de Dr. Ariel e indeferimento das diárias para o Assessor, em função da Promotoria de Justiça de Cícero Dantas possuir servidor para auxiliar Dr. Ariel.

O trigésimo nono item da pauta, Processo Eletrônico SEI Nº. 19.09.00855.0018130/2021-52, se refere a solicitação de autorização de 06 diárias e meia para Dr. Ariomar José Figueiredo da Silva, Titular do Tribunal do Júri, bem como autorização para registro no Sistema, em razão de bloqueio por exceder o limite de 04 diárias, em função do seu deslocamento para Comarca de Santa Rita de Cássia, no período de 23 de outubro a 29 de outubro de 2021, para atuar nas Sessões do Tribunal do Júri que serão realizadas nos dias 25 e 27 de outubro de 2021. Dr. Ariomar justifica que o mencionado deslocamento será realizado em veículo próprio e no dia 23 de outubro de 2021 (sábado), em razão da distância de Salvador para Santa Rita de Cássia, aproximadamente 1010 Km. Esclareceu Dr. Ricardo que Dr. Ariomar tem sido requisitado pelos colegas para realização de júri no Interior. Esclareceu ainda Dr. Ricardo que, além da presente solicitação, Dr. Ariomar foi requisitado para Poções, Ruy Barbosa e Vitória da Conquista. Acrescentou Dr. Ricardo mais algumas informações, contribuindo com a avaliação do pleito em questão. Dra. Cleonice e Dr. Ricardo fizeram suas explanações, votando pela aprovação. O Superintendente acompanhou o voto de Dra. Cleonice e Dr. Ricardo.

O quadragésimo item da pauta, Processo Eletrônico SEI Nº. 19.09.02350.0017198/2021-64, se refere a solicitação registrada pela Coordenação de Execução Orçamentária Administrativa para autorização de pagamento de 02 diárias e meia para Dr. Ariomar José Figueiredo da Silva, Titular da Promotoria do Júri, face a realização de auxílio/colaboração na Promotoria de Justiça de Poções, de 14 a 16 de setembro de 2021, bem como autorização para pagamento de 01 diária e meia para Dra. Daniela de Almeida, Titular de Encruzilhada, face a necessidade de realização de substituição na Promotoria de Justiça de Candido Sales.

O quadragésimo primeiro item da pauta, Processo Eletrônico SEI Nº. 19.09.02350.0017197/2021-57, se refere a solicitação registrada pela Coordenação de Execução Orçamentária Administrativa para apreciação pelo Comitê de Repactuação Orçamentária das diárias de membros e servidores. Esclareceu o Superintendente que consta no referido processo, a solicitação de 01 diária para o motorista Benites Dantas da Cruz Junior, lotado em Juazeiro, face a necessidade de condução de Dr. Raimundo Nonato Santana Moinhos, de 06 a 07 de outubro de 2021, para Promotoria de Substituição em Sento Sé; 02 meias diárias para Dr. Dioneles Leone Santana Filho, Titular de Itabuna, face a necessidade de substituição na Promotoria de Justiça de Itajuípe, nos dias 13 de setembro e 04 de outubro de 2021; meia diária para Dr. Felipe Otaviano Ranauro, Titular de Santo Antônio de Jesus, face a necessidade de substituição na Promotoria de Justiça de Valença, no dia 14 de outubro de 2021; Meia diária para Dr. Gilberto Ribeiro de Campos, Titular de Teixeira de Freitas, face a necessidade de substituição na Promotoria de Justiça de Prado, no dia 24 de setembro de 2021, bem como 04 diárias para o mês de outubro/2021; 04 diárias para Dr. Luciano Valadares Garcia, Titular de Lauro de Freitas, face a necessidade de substituição na Promotoria de Justiça de Livramento de Nossa Senhora durante o mês de outubro; meia diária para Dr. Marcelo dos Santos Carneiro Porto, Titular de Bom Jesus da Lapa, face a necessidade de substituição na Promotoria de Justiça de Riacho de Santana, no dia 07 de outubro de 2021; meia diária para Dr. Márcio Henrique Pereira de Oliveira, Titular de Juazeiro, face a necessidade de substituição na Promotoria de Justiça de Curaçá, no dia 07 de outubro de 2021; meia diária para o servidor Orlando Dias dos Santos Júnior, lotado na Promotoria de Justiça de Belo Campo, face a necessidade de acompanhamento de Dra. Guiomar Miranda de Oliveira Melo, na Promotoria de Justiça de Substituição de Condeúba, no dia 05 de outubro de 2021; 01 diária para Dra. Patrícia Camilo Caetano Silva, Titular de Casa Nova, face a necessidade de substituição na Promotoria de Justiça de Remanso, de 22 a 23 de outubro de 2021.

O quadragésimo segundo item da pauta, Processo Eletrônico SEI Nº. 19.09.00855.0017869/2021-68, se refere a solicitação de autorização de meia diária para Dr. Gilberto Ribeiro de Campos, Titular de Teixeira de Freitas, em razão do seu deslocamento para Comarca de Substituição em Prado, no dia 01 de outubro de 2021, que acabou ultrapassando o limite estabelecido de 04 diárias, durante o mês de outubro/2021.

O quadragésimo terceiro item da pauta, Processo Eletrônico SEI Nº. 19.09.02350.0017878/2021-71, se refere a solicitação registrada pela Coordenação de Execução Orçamentária Administrativa para apreciação pelo Comitê de Repactuação Orçamentária das diárias de membros e servidores. Esclareceu o Superintendente que consta no referido processo a solicitação de 02 diárias para Dr. Raimundo Nonato Santana Moinhos, Titular de Juazeiro, face a necessidade de substituição na Promotoria de Justiça de Sento Sé, durante o mês de outubro/2021; 01 diária para Dr. Rodolfo Fontenele Belchior Cabral, Titular de Xique-Xique, face a necessidade de auxílio/colaboração na Promotoria de Justiça de Lapão, de 18 a 19 de outubro de 2021; 01 diária para Dr. Rodolfo Ribeiro de La Fuente, Titular de Jacobina, face a necessidade de substituição na Promotoria de Justiça de Miguel Calmon, de 13 a 14 de outubro de 2021; 02 diárias para Dr. Romeu Gonsalves Coelho Filho, Titular de Irecê, face a necessidade de auxilio/colaboração em Salvador - 1ª Vara do Júri - Portaria 1116/2021, de 20 a 22 de outubro de 2021; meia diária para servidora Sheila Maria da Rocha, lotada em Vitória da Conquista, face a necessidade de acompanhamento de Dra. Guiomar Miranda de Oliveira Melo, na Promotoria de Justiça de Substituição de Condeúba, no dia 14 de setembro de 2021; meia diária para o motorista Thiago Costa de Farias, lotado em Itaberaba, face a necessidade de entrega de notificações, no dia 19 de outubro de 2021, na Promotoria de Justiça de Castro Alves; meia diária para Dr. Thyego de Oliveira Matos, Titular de Itaberaba, face a necessidade de substituição na Promotoria de Justiça de Iaçu, no dia 20 de outubro de 2021; meia diária para Dr. Victor Freitas Leite Barros, Titular de Amargosa, face a necessidade de substituição na Promotoria de Justiça de Muritiba, no dia 05 de outubro de 2021; meia diária para o motorista Wilson de Jesus de Souza, lotado em Santo Antônio de Jesus, face a necessidade de condução de Dr. Julimar Barreto Ferreira de Santo Antônio de Jesus para Salvador, no dia 13 de outubro de 2021; 01 diária para o motorista Milton Romualdo de Sousa, lotado em Juazeiro, face a necessidade de condução de Dr. Raimundo Nonato Santana Moinhos, de 14 a 15 de setembro de 2021, para Promotoria de Substituição em Sento Sé.

O quadragésimo quarto item da pauta, Processo Eletrônico SEI Nº. 19.09.02350.0017877/2021-64, se refere a solicitação registrada pela Coordenação de Execução Orçamentária Administrativa para apreciação pelo Comitê de Repactuação Orçamentária das diárias de membros e servidores. Esclareceu o Superintendente que consta no processo a solicitação de meia diária para Dr. Guilherme Abrante Cardoso de Moraes, Titular de Correntina, face a necessidade de substituição na Promotoria de Justiça de Cocos, no dia 18 de outubro de 2021; 01 diária para Dr. Isaias Marcos Borges Carneiro, Titular de Ubaíra, face a

necessidade de substituição na Promotoria de Justiça de Santa Inês, de 04 a 05 de novembro de 2021; 01 diária e meia para Dr. Ivan Carlos Novaes Machado, Titular de Irecê, face a necessidade de substituição na Promotoria de Justiça de Central, durante o mês de outubro/2021; meia diária para Dr. Marcelo dos Santos Carneiro Porto, Titular de Bom Jesus da Lapa, face a necessidade de substituição na Promotoria de Justiça de Riacho de Santana, no dia 20 de outubro de 2021; 01 diária para Dr. Marco Aurélio Rubick da Silva, Titular de Caculé, face a necessidade de substituição na Promotoria de Justiça de Tanque Novo, no dia 14 de outubro de 2021; 01 diária para o servidor Michael John Dias Freire, lotado em Guanambi, face a necessidade de realização de serviços técnicos/administrativos na Promotoria de Justiça de Carinhanha, solicitados por Dr. Ailson de Almeida Marques, durante o mês de outubro/2021; meia diária para Dra. Patrícia Camilo Caetano Silva, Titular de Casa Nova, face a necessidade de substituição na Promotoria de Justiça de Sobradinho, no dia 25 de outubro de 2021; 01 diária para Dra. Patrícia Camilo Caetano Silva, Titular de Casa Nova, face a necessidade de substituição na Promotoria de Justiça de Remanso, de 28 a 29 de outubro de 2021; meia diária para Dr. Pedro Nogueira Coelho, Titular de Ilhéus, face a necessidade de substituição na Promotoria de Justiça de Uruçuca, no dia 19 de outubro de 2021.

O quadragésimo quinto item da pauta, Processo Eletrônico SEI Nº. 19.09.02350.0017875/2021-50, se refere a solicitação registrada pela Coordenação de Execução Orçamentária Administrativa para apreciação pelo Comitê de Repactuação Orçamentária das diárias de membros e servidores. Esclareceu o Superintendente que consta no processo a solicitação de 03 diárias e meia para Dr. Ailson de Almeida Marques, Titular de Amargosa, face a necessidade de substituição na Promotoria de Justiça de Carinhanha, de 22 a 25 de novembro de 2021; 01 diária para o motorista André de Andrade Vieira, lotado em Guanambi, face a necessidade de condução do servidor Michael John Freire para realização de serviços técnicos/administrativos na Promotoria de Justiça de Carinhanha, solicitados por Dr. Ailson de Almeida Marques, durante o mês de outubro/2021; 01 diária e meia para Dr. André Luís Lavigne Mota, Titular de Salvador, devido a sua participação junto a Procuradora-Geral de Justiça na Audiência com o Conselheiro Mario Maia – CNJ, bem como de outras reuniões institucionais, de 06 a 07 de outubro de 2021, em Brasília/DF; 02 diárias para Dr. Aviner Rocha Santos, Titular de Itaberaba, face a necessidade de auxilio/colaboração em Salvador - 1ª Vara do Júri - Portaria 1116/2021, de 20 a 22 de outubro de 2021; meia diária para Dr. Carlos André Milton Pereira, Titular de Santo Estevão, face a necessidade de substituição em Castro Alves, no dia 28 de outubro de 2021; meia diária para o servidor Edvan Silva dos Santos, lotado em Correntina, face a necessidade de acompanhamento de Dr. Guilherme Abrante Cardoso de Moraes, na Promotoria de Justiça de Substituição de Cocos, no dia 18 de outubro de 2021; meia diária para o motorista Fabiano Américo de Amorim, lotado em Juazeiro, face a necessidade de condução de Dr. Márcio Henrique Pereira de Oliveira, na Promotoria de Justiça de Substituição de Curaçá, no dia 07 de outubro de 2021; 01 diária para Dr. Felipe Otaviano Ranauro, Titular de Santo Antônio de Jesus, face a necessidade de substituição em Valença, durante o mês de outubro/2021; meia diária para o motorista Fernando César Moleiro Lima, lotado em Bom Jesus da Lapa, face a necessidade de condução de Dr. Marcelo dos Santos Carneiro Porto, de Bom Jesus da Lapa para Riacho de Santana, no dia 07 de outubro de 2021; meia diária para o motorista Fernando César Moleiro Lima, lotado em Bom Jesus da Lapa, face a necessidade de condução de Dra. Jessica Camille Tojal, de Bom Jesus da Lapa para Paratinga e Serra do Ramalho, no dia 18 de outubro de 2021; meia diária para Dr. Fernando Rodrigues de Assis, Titular de Brumado, face a necessidade de substituição em Ituaçu, no dia 14 de outubro de 2021.

Após a leitura e avaliação de todos os itens, relativos as diárias, Dra. Cleonice, Dr. Ricardo e o Superintendente, votaram pela aprovação em bloco do vigésimo nono ao quadragésimo quinto item da pauta, com ressalva apenas para o trigésimo oitavo item, pois foram aprovadas apenas as diárias de Dr. Ariel e indeferimento das diárias para o Assessor, em função da Promotoria de Justiça de Cícero Dantas possuir servidor para auxiliar Dr. Ariel.

Encerrada a avaliação dos itens formais da pauta, o Superintendente comunicou que serão apreciados com celeridade 04 itens, na Sessão “O que Ocorrer”.

Discorreu o Superintendente que o quadragésimo sexto item, se refere a solicitação de autorização para pagamento de diárias aos servidores que realizarão o inventário de 2021 nas Unidades da Instituição, inclusive nas Promotorias do Interior do Estado. Esclareceu o Superintendente que foi emitido um comunicado geral para realização do inventário de bens permanentes e assim como foi realizado no ano passado é necessário a aprovação prévia do comitê para solicitação de diárias, pois é programado um roteiro mais próximo possível e a realização do inventário é sempre efetuada por servidor diverso da sua unidade de lotação. Finalizou o Superintendente a sua explanação, requerendo a colaboração do Comitê para aprovação prévia da solicitação das diárias com posterior prestação de contas ao Comitê. Submeteu o Superintendente, a presente solicitação para avaliação, iniciando por Dra. Cleonice. Dra. Cleonice informou que não se opõe e que vota pela aprovação. Dr. Ricardo e o Superintendente acompanharam o voto de Dra. Cleonice.

O próximo item, quadragésimo sétimo item, Processo Eletrônico SEI Nº. 19.09.02385.0013885/2021-52, oriundo do CEOSP/UMPE, relativo à solicitação de liberação de recursos destinados à realização de visitas técnicas para atualização do diagnóstico do sistema prisional do Estado da Bahia pela equipe técnica da UMEP, no valor de R$ 35.000,00, se refere apenas a necessidade de ratificar que a solicitação de liberação do mencionado recurso destina-se à realização de visitas técnicas, compreendendo o pagamento de diárias e passagens aéreas. Dra. Cleonice reforçou que precisa do relatório dessas visitas, pois está sendo cobrada pelo CNMP – Conselho Nacional do Ministério Público.

O penúltimo item, quadragésimo oitavo, Processo SEI Nº. 19.09.02693.0018266/2021-90, encaminhado pela Secretaria Geral, se refere ao requerimento de auxílio para Promotoria de Justiça de Formosa do Rio Preto, efetuado pela Dra. Caroline Maronita Stange, Promotoria de Justiça Substituta em exercício na Promotoria de Justiça de Formosa do Rio Preto. Pontuou o Superintendente que consta no processo parecer favorável da Corregedoria-Geral. Dra. Cleonice e Dr. Ricardo fizeram suas explanações, votando pela aprovação. O Superintendente acompanhou o voto de Dra. Cleonice, bem como Dr. Ricardo.

O último item, quadragésimo nono, por enquanto sem número de processo, se refere a solicitação de realização de mutirão do Apoio a 2ª Instância. O Superintendente solicitou aprovação da presente solicitação, pois, em caráter emergencial, de acordo com provocação de Dra. Cleonice, através de e-mail e reunião realizada com a servidora Ana Paula Mota será realizado um mutirão para o Apoio a 2ª Instância, devido ao acúmulo de processos e que esse mutirão ocorrerá durante dois finais de semana, gerando um custo em torno de R$ 4.800,00 com pagamento de horas extras. Reforçou o Superintendente que a presente solicitação foi efetivada, em caráter excepcional, para que baixe o passivo dos processos do Apoio a 2ª Instância e que o mutirão fora realizado nos dias 09 e 11 de outubro de 2021, bem como será realizado no dia 23 de outubro de 2021, com o custo estimado de R$ 4.800,00, visando sanar o acumulo desses processos. Abriu para discussão o Superintendente, iniciando por Dra. Cleonice. Dra. Cleonice fez a sua explanação, votando pela aprovação. Dr. Ricardo e o Superintendente acompanharam o voto de Dra. Cleonice.

Nada mais tendo a discutir, deu-se por encerrada a reunião.

Salvador, 20 de outubro de 2021.

Dra. Cleonice Souza de Lima
Corregedora Geral

Dr. Ricardo Assis
Secretário-Geral Adjunto

Frederico Welington Silveira Soares

Superintendente de Gestão Administrativa

Documento assinado eletronicamente por **Frederico Welington Silveira Soares** em 26/10/2021, às 09:22, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Pedro Maia Souza Marques** em 26/10/2021, às 14:34, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Ricardo de Asis andrade** em 27/10/2021, às 10:10, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.sistemas.mpba.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0221020** e o código CRC **E6523225**.

MINISTÉRIO PÚBLICO
DO ESTADO DA BAHIA

DESPACHO

- Autorizado pela Procuradoria Geral de Justiça, nos termos da manifestação do Comitê de Repactuação Orçamentária.
- Encaminhe-se o presente expediente à Superintendência de Gestão Administrativa para conhecimento e adoção das providências pertinentes, inclusive quanto às comunicações necessárias.

NORMA ANGÉLICA REIS CARDOSO CAVALCANTI
Procuradora-Geral de Justiça

Documento assinado eletronicamente por **Norma Angélica Reis Cardoso Cavalcanti** em 03/11/2021, às 12:25, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.sistemas.mpba.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0225319** e o código CRC **9893C7D7**.

MINISTÉRIO PÚBLICO
DO ESTADO DA BAHIA

DESPACHO

Considerando que a Procuradoria-Geral de Justiça autorizou, nos termos da manifestação do Comitê de Repactuação Orçamentária, a Dispensa de Licitação, em favor da empresa **STEFANINI RAFAEL SEGURANÇA E DEFESA S.A** , no valor total de **R$ 8.202,67 (oito mil duzentos e dois reais e sessenta e sete centavos)**, visando à prestação de serviços técnicos, na área de tecnologia da informação, para a varredura de vulnerabilidades e testes de intrusão - PENTEST em uma aplicação *Web* (Voto Digital), no formato *Black-Box*, encaminhe-se o presente expediente à DCCL/Coordenação de Elaboração e Acompanhamentos de Contratos e Convênios para ciência e adoção das providências cabíveis.

Documento assinado eletronicamente por **Frederico Welington Silveira Soares** em 03/11/2021, às 1: 5 f , con.orme artº 1l , "", bLb, da 4ei 11ºf 19/2006º

A autenticidade do documento pode ser con.erida no site https5/seiºsistemasºmpLaºmpºLr/sei/controlador_externoºphp?acao=documento_con.erir&id_orgao_acesso_externo=0 in.ormando o código veri.icador **0226637** e o código CRC **BE25D130º**

MINISTÉRIO PÚBLICO
DO ESTADO DA BAHIA

CERTIDÃO

Certificamos, para os devidos fins, que procedemos à consulta da situação da empresa contratada, **STEFANINI RAFAEL SEGURANÇA E DEFESA S.A,** CNPJ **24.691.488/0001-09,** e de seus respectivos sócios, no que diz respeito à eventual aplicação de sanção administrativa de impedimento ou suspensão do direito de contratar com a Administração Pública (docs anexos - 0227439), não tendo sido encontrados registros neste sentido. Ressaltamos, no que diz respeito a sanções eventualmente aplicadas por este Ministério Público Estadual, que após consulta à publicação relativa a fornecedores sancionados através do link https://www.mpba.mp.br/area/licitacao/biblioteca/1732, igualmente não foram encontradas restrições à referida empresa.

Coordenação de Elaboração e Acompanhamento de Contratos e Convênios
Diretoria de Contratos, Convênios e Licitações

Documento assinado eletronicamente por **Milena Maria Cardoso do Nascimento** em 03/99/20291, s 0à:421conforme art. 9º1III1"b"1da Lei 99.39à/2006.

A autenticidade do documento pode ser conferida no site https://sei.sistemas.mpba.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0227436** e o código CRC **91F3C16D**.

TRIBUNAL DE CONTAS DA UNIÃO

Consulta Consolidada de Pessoa Jurídica

Este relatório tem por objetivo apresentar os resultados consolidados de consultas eletrônicas realizadas diretamente nos bancos de dados dos respectivos cadastros. A responsabilidade pela veracidade do resultado da consulta é do Órgão gestor de cada cadastro consultado. A informação relativa à razão social da Pessoa Jurídica é extraída do Cadastro Nacional da Pessoa Jurídica, mantido pela Receita Federal do Brasil.

Consulta realizada em: 04/11/2021 09:20:42

Informações da Pessoa Jurídica:

Razão Social: **STEFANINI RAFAEL SEGURANCA E DEFESA S.A.**
CNPJ: **24.691.488/0001-09**

Resultados da Consulta Eletrônica:

Órgão Gestor: **TCU**
Cadastro: **Licitantes Inidôneos**
Resultado da consulta: **Nada Consta**

Para acessar a certidão original no portal do órgão gestor, clique AQUI.

Órgão Gestor: **CNJ**
Cadastro: **CNIA - Cadastro Nacional de Condenações Cíveis por Ato de Improbidade Administrativa e Inelegibilidade**
Resultado da consulta: **Nada Consta**

Para acessar a certidão original no portal do órgão gestor, clique AQUI.

Órgão Gestor: **Portal da Transparência**
Cadastro: **Cadastro Nacional de Empresas Inidôneas e Suspensas**
Resultado da consulta: **Nada Consta**

Para acessar a certidão original no portal do órgão gestor, clique AQUI.

Órgão Gestor: **Portal da Transparência**
Cadastro: **CNEP - Cadastro Nacional de Empresas Punidas**
Resultado da consulta: **Nada Consta**

Para acessar a certidão original no portal do órgão gestor, clique AQUI.

Obs: A consulta consolidada de pessoa jurídica visa atender aos princípios de simplificação e

racionalização de serviços públicos digitais. Fundamento legal: Lei nº 12.965, de 23 de abril de 2014, Lei nº 13.460, de 26 de junho de 2017, Lei nº 13.726, de 8 de outubro de 2018, Decreto nº 8.638 de 15, de janeiro de 2016.

TRIBUNAL DE CONTAS DA UNIÃO

CERTIDÃO NEGATIVA

DE

LICITANTES INIDÔNEOS

(Válida somente com a apresentação do CPF)

Nome completo: **MARCO ANTONIO SILVA STEFANINI**

CPF/CNPJ: [redacted]

O Tribunal de Contas da União CERTIFICA que, na presente data, o (a) requerente acima identificado(a) NÃO CONSTA da relação de responsáveis inidôneos para participar de licitação na administração pública federal, por decisão deste Tribunal, nos termos do art. 46 da Lei nº 8.443/92 (Lei Orgânica do TCU).

Não constam da relação consultada para emissão desta certidão os responsáveis ainda não notificados do teor dos acórdãos condenatórios, aqueles cujas condenações tenham tido seu prazo de vigência expirado, bem como aqueles cujas apreciações estejam suspensas em razão de interposição de recurso com efeito suspensivo ou de decisão judicial.

Certidão emitida às 09:20:57 do dia 04/11/2021, com validade de trinta dias a contar da emissão.

A veracidade das informações aqui prestadas podem ser confirmadas no sítio https://contas.tcu.gov.br/ords/f?p=INABILITADO:5

Código de controle da certidão: YDND041121092057

Atenção: qualquer rasura ou emenda invalidará este documento.

TRIBUNAL DE CONTAS DA UNIÃO

CERTIDÃO NEGATIVA

DE

LICITANTES INIDÔNEOS

(Válida somente com a apresentação do CPF)

Nome completo: **MARIA MAGALI BREDARIOL**

CPF/CNPJ [redacted]

O Tribunal de Contas da União CERTIFICA que, na presente data, o (a) requerente acima identificado(a) NÃO CONSTA da relação de responsáveis inidôneos para participar de licitação na administração pública federal, por decisão deste Tribunal, nos termos do art. 46 da Lei nº 8.443/92 (Lei Orgânica do TCU).

Não constam da relação consultada para emissão desta certidão os responsáveis ainda não notificados do teor dos acórdãos condenatórios, aqueles cujas condenações tenham tido seu prazo de vigência expirado, bem como aqueles cujas apreciações estejam suspensas em razão de interposição de recurso com efeito suspensivo ou de decisão judicial.

Certidão emitida às 09:21:12 do dia 04/11/2021, com validade de trinta dias a contar da emissão.

A veracidade das informações aqui prestadas podem ser confirmadas no sítio https://contas.tcu.gov.br/ords/f?p=INABILITADO:5

Código de controle da certidão: FHER041121092112

Atenção: qualquer rasura ou emenda invalidará este documento.

TRIBUNAL DE CONTAS DA UNIÃO

CERTIDÃO NEGATIVA

DE

LICITANTES INIDÔNEOS

(Válida somente com a apresentação do CPF)

Nome completo: **MARIA DAS GRACAS VUOLO SAJOVIC STEFANINI**

CPF/CNPJ: [redacted]

O Tribunal de Contas da União CERTIFICA que, na presente data, o (a) requerente acima identificado(a) NÃO CONSTA da relação de responsáveis inidôneos para participar de licitação na administração pública federal, por decisão deste Tribunal, nos termos do art. 46 da Lei nº 8.443/92 (Lei Orgânica do TCU).

Não constam da relação consultada para emissão desta certidão os responsáveis ainda não notificados do teor dos acórdãos condenatórios, aqueles cujas condenações tenham tido seu prazo de vigência expirado, bem como aqueles cujas apreciações estejam suspensas em razão de interposição de recurso com efeito suspensivo ou de decisão judicial.

Certidão emitida às 09:21:27 do dia 04/11/2021, com validade de trinta dias a contar da emissão.

A veracidade das informações aqui prestadas podem ser confirmadas no sítio https://contas.tcu.gov.br/ords/f?p=INABILITADO:5

Código de controle da certidão: 4THA041121092127

Atenção: qualquer rasura ou emenda invalidará este documento.

TRIBUNAL DE CONTAS DA UNIÃO

CERTIDÃO NEGATIVA

DE

LICITANTES INIDÔNEOS

(Válida somente com a apresentação do CPF)

Nome completo: **AILTON BARBERINO DO NASCIMENTO FILHO**

CPF/CNPJ: [redacted]

O Tribunal de Contas da União CERTIFICA que, na presente data, o (a) requerente acima identificado(a) NÃO CONSTA da relação de responsáveis inidôneos para participar de licitação na administração pública federal, por decisão deste Tribunal, nos termos do art. 46 da Lei nº 8.443/92 (Lei Orgânica do TCU).

Não constam da relação consultada para emissão desta certidão os responsáveis ainda não notificados do teor dos acórdãos condenatórios, aqueles cujas condenações tenham tido seu prazo de vigência expirado, bem como aqueles cujas apreciações estejam suspensas em razão de interposição de recurso com efeito suspensivo ou de decisão judicial.

Certidão emitida às 09:29:22 do dia 04/11/2021, com validade de trinta dias a contar da emissão.

A veracidade das informações aqui prestadas podem ser confirmadas no sítio https://contas.tcu.gov.br/ords/f?p=INABILITADO:5

Código de controle da certidão: S4XN041121092922

Atenção: qualquer rasura ou emenda invalidará este documento.

Certidão Negativa

Certifico que nesta data (04/11/2021 às 09:22) NÃO CONSTA no Cadastro Nacional de Condenações Cíveis por Ato de Improbidade Administrativa e Inelegibilidade registros de condenação com trânsito em julgado ou sanção ativa quanto ao CNPJ nº 24.691.488/0001-09.

A condenação por atos de improbidade administrativa não implica automático e necessário reconhecimento da inelegibilidade do condenado.
Para consultas sobre inelegibilidade acesse portal do TSE em http://divulgacandcontas.tse.jus.br/

Esta certidão é expedida gratuitamente. Sua autenticidade pode ser por meio do número de controle 6183.D06D.3F04.C525 no seguinte endereço: https://www.cnj.jus.br/improbidade_adm/autenticar_certidao.php

Anexo Consulta - Stefanini (0227439) SEI 19.09.02684.0011790/2021-22 / pg. 749

Certidão Negativa

Certifico que nesta data (04/11/2021 às 09:22) NÃO CONSTA no Cadastro Nacional de Condenações Cíveis por Ato de Improbidade Administrativa e Inelegibilidade registros de condenação com trânsito em julgado ou sanção ativa quanto ao CPF nº [redacted].

A condenação por atos de improbidade administrativa não implica automático e necessário reconhecimento da inelegibilidade do condenado.
Para consultas sobre inelegibilidade acesse portal do TSE em http://divulgacandcontas.tse.jus.br/

Esta certidão é expedida gratuitamente. Sua autenticidade pode ser por meio do número de controle 6183.D07B.47FB.E539 no seguinte endereço: https://www.cnj.jus.br/improbidade_adm/autenticar_certidao.php

Anexo Consulta - Stefanini (0227439) SEI 19.09.02684.0011790/2021-22 / pg. 750

Certidão Negativa

Certifico que nesta data (04/11/2021 às 09:22) NÃO CONSTA no Cadastro Nacional de Condenações Cíveis por Ato de Improbidade Administrativa e Inelegibilidade registros de condenação com trânsito em julgado ou sanção ativa quanto ao CPF nº [redacted].

A condenação por atos de improbidade administrativa não implica automático e necessário reconhecimento da inelegibilidade do condenado.
Para consultas sobre inelegibilidade acesse portal do TSE em http://divulgacandcontas.tse.jus.br/

Esta certidão é expedida gratuitamente. Sua autenticidade pode ser por meio do número de controle 6183.D088.178C.1552 no seguinte endereço: https://www.cnj.jus.br/improbidade_adm/autenticar_certidao.php

Anexo Consulta - Stefanini (0227439) SEI 19.09.02684.0011790/2021-22 / pg. 751

Certidão Negativa

Certifico que nesta data (04/11/2021 às 09:22) NÃO CONSTA no Cadastro Nacional de Condenações Cíveis por Ato de Improbidade Administrativa e Inelegibilidade registros de condenação com trânsito em julgado ou sanção ativa quanto ao CPF nº [redacted].

A condenação por atos de improbidade administrativa não implica automático e necessário reconhecimento da inelegibilidade do condenado.
Para consultas sobre inelegibilidade acesse portal do TSE em http://divulgacandcontas.tse.jus.br/

Esta certidão é expedida gratuitamente. Sua autenticidade pode ser por meio do número de controle 6183.D098.0857.3568 no seguinte endereço: https://www.cnj.jus.br/improbidade_adm/autenticar_certidao.php

Anexo Consulta - Stefanini (0227439) SEI 19.09.02684.0011790/2021-22 / pg. 752

Certidão Negativa

Certifico que nesta data (04/11/2021 às 09:23) NÃO CONSTA no Cadastro Nacional de Condenações Cíveis por Ato de Improbidade Administrativa e Inelegibilidade registros de condenação com trânsito em julgado ou sanção ativa quanto ao CPF nº [redacted].

A condenação por atos de improbidade administrativa não implica automático e necessário reconhecimento da inelegibilidade do condenado.
Para consultas sobre inelegibilidade acesse portal do TSE em http://divulgacandcontas.tse.jus.br/

Esta certidão é expedida gratuitamente. Sua autenticidade pode ser por meio do número de controle 6183.D0A5.CC35.6581 no seguinte endereço: https://www.cnj.jus.br/improbidade_adm/autenticar_certidao.php

Anexo Consulta - Stefanini (0227439) SEI 19.09.02684.0011790/2021-22 / pg. 753

FILTROS APLICADOS:

CPF / CNPJ: 24691488000109 [redacted]

LIMPAR

Data da consulta: 04/11/2021 08:42:03
Data da última atualização: 03/11/2021 18:00:05

DETALHAR	CNPJ/CPF DO SANCIONADO	NOME DO SANCIONADO	UF DO SANCIONADO	ÓRGÃO/ENTIDADE SANCIONADORA	TIPO DA SANÇÃO	DATA DE PUBLICAÇÃO DA SANÇÃO	QUANTIDADE
Nenhum registro encontrado							

Comprasnet.Ba

Relação de Fornecedores Impedidos de Licitar e Contratar

Natureza Juridica: Pessoa Jurídica
CPF/CNPJ: 24691488000109
Tipo de Suspensao: Todas

Razão Social	CNPJ/CPF	Portaria	Prazo	Expiração

Voltar

Governo do Estado da Bahia

Comprasnet.Ba

Relação de Fornecedores Impedidos de Licitar e Contratar

Natureza Juridica: Pessoa Física
CPF/CNPJ: [redacted]
Tipo de Suspensao: Todas

Razão Social	CNPJ/CPF	Portaria	Prazo	Expiração

Voltar

Governo do Estado da Bahia

Comprasnet.Ba

Relação de Fornecedores Impedidos de Licitar e Contratar

Natureza Juridica: Pessoa Física
CPF/CNPJ: [redacted]
Tipo de Suspensao: Todas

Razão Social	CNPJ/CPF	Portaria	Prazo	Expiração

Voltar

Governo do Estado da Bahia

Comprasnet.Ba

Relação de Fornecedores Impedidos de Licitar e Contratar

Natureza Juridica: Pessoa Física
CPF/CNPJ: [redacted]
Tipo de Suspensao: Todas

Razão Social	CNPJ/CPF	Portaria	Prazo	Expiração

Voltar

Governo do Estado da Bahia

Comprasnet.Ba

Relação de Fornecedores Impedidos de Licitar e Contratar

Natureza Juridica: Pessoa Física
CPF/CNPJ: [redacted]
Tipo de Suspensao: Todas

Razão Social	CNPJ/CPF	Portaria	Prazo	Expiração

Voltar

Governo do Estado da Bahia

MINISTÉRIO PÚBLICO
DO ESTADO DA BAHIA

DESPACHO

Considerando a conclusão do procedimento adninistrativo cabível, encaminhamos o expediente para a unidade demandante para que seja diligenciada a coleta de assinatura da contratada. Para tanto, anexamos ao presente, em formato editável, o arquivo final a ser assinado, devidamente numerado.

Esclarecemos, no ensejo, que a assinatura do contrato deverá ocorrer, alternativamente (e conforme ordem de prioridade) da seguinte forma:

1. Preferencialmente, o documento poderá ser assinado VIA SEI/MPBA (Sistema eletrônico de informações - MPBA).Nesta hipótese será necessário atender às seguintes etapas:

   a) 1º Preencher o cadastro de usuário externo:

   https://sei.sistemas.mpba.mp.br/sei/controlador_externo.php?acao=usuario_externo_logar&acao_origem=usuario_externo_enviar_cadastro&id_orgao_acesso_externo=0

   b) 2º seguir as orientações descritas no link para encaminhamento da documentação:

   https://portalsei.mpba.mp.br/acesso-externo/local-de-entrega-das-documentacoes/

2. Alternativamente, o documento poderá ser assinado digitalmente. **Nesta hipótese, faz-se necessário que a assinatura seja aposta em todas as páginas do documento e, ainda, que seja encaminhado, também, o certificado de validação da assinatura digital.**

3. Por fim, e excepcionalmente, o documento poderá ser assinado fisicamente, em 02 (duas) vias, as quais, após assinatura, deverão ser enviadas à esta Coordenação para coleta de assinatura do Superintendente de Gestão Administrativa.

Após, retorne-se o expediente, com as vias assinadas, para que sejam adotadas as demais providências cabíveis.

Documento assinado eletronicamente por **Paula Souza de Paula** em 04/11/2021, às 10:10, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.sistemas.mpba.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0227507** e o código CRC **87701666**.

MINISTÉRIO PÚBLICO
DO ESTADO DA BAHIA

CONTRATO PARA PRESTAÇÃO DE SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO, QUE ENTRE SI CELEBRAM O MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA E A EMPRESA STEFANINI RAFAEL SEGURANÇA E DEFESA S.A, NA FORMA ABAIXO:

CONTRATO Nº xxx/202x 1SGA

O **MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA**, CNPJ nº 04.142.491/0001-66, com sede situada à 5ª Avenida, 750, Centro Administrativo da Bahia - CAB, Salvador - BA, neste ato representado, mediante Ato de Delegação nº 70/2014, pelo Superintendente de Gestão Administrativa **F-rer-dc orWngcl SdWrd-v Scv-ra**, doravante denominado **CONTRATANTE**, e a **EMPRESA STEFANINI RAFAEL SEGURANÇA E DEFESA S.A.**, CNPJ nº 24.691.488/0001-09, estabelecida à Avenida Eusebio Matoso, nº 1375, Andar 8, Salas 801 e 802, Butantã, CEP 05423-905, São Paulo/SP, representada por sua **-rs-rarlgvlgr WnvW**Sra. **Mv-dv MvnvWB-rev-dcW**inscrito no CPF/MF nº [redacted], doravante denominada **CONTRATADA**, com supedâneo no quanto disposto na Lei Estadual-BA nº 9.433/2005, na Medida Provisória nº 961 de maio de 2020, e, ainda, observado o constante no processo de Dispensa de Licitação nº 004/2021-DTI protocolado sob o nº 19.09.02684.0011790/2021-22, o qual integra este instrumento independentemente de transcrição, **CELEBRAM** o presente Contrato, mediante as cláusulas e condições seguintes:

CLpUSULA PRIMEIRA 1DO OBÁETO

1.1 Constitui objeto do presente contrato a prestação de serviços técnicos, na área de tecnologia da informação, para a varredura de vulnerabilidades e testes de intrusão – PENTEST – na aplicação WEB VOTO DIGITAL, no formato Black Box, nos termos e condições do presente instrumento.

CLpUSULA SEGUNDA J DO REGIME DE EXECUÇÃO, DA ENTREGA E DO RECEBIMENTO

2.1 O regime de execução do contrato é o de Empreitada Indireta por preço global;

2.2 O **CONTRATANTE** convocará a **CONTRATADA** para retirar a nota de empenho no prazo de até 05 (cinco) dias contados da data da notificação, a ser efetivada, preferencialmente, por e-mail;

Anexo Contrato 111-2021 (0227530) SEI 19.09.02684.0011790/2021-22 / pg. 761

2.2.1 As comprovações da convocação e da entrega/retirada da nota de empenho poderão ocorrer por quaisquer dos seguintes meios: por meio eletrônico (através de confirmação de recebimento de e-mail), aposição de assinatura (para retirada presencial) ou por Aviso de Recebimento dos correios (quando a entrega for via postal).

2.2.2 A **CONTRATADA** poderá solicitar a prorrogação do prazo para retirada/recebimento da nota de empenho, por igual período ao original, por motivo justo e aceito pela Administração, nos termos do art. 124, § 4º, da Lei Estadual – BA nº 9433/2005.

2.3 O Teste de Intrusão/Penetração (PENTEST) compreende o teste de Invasão externa e tem como objetivo principal identificar, possíveis vulnerabilidades na aplicação WEB VOTO DIGITAL da **CONTRATANTE**, observando-se ainda:

2.3.1 Os serviços objeto deste instrumento envolvem o uso de técnicas e ferramentas para tentar o acesso privilegiado aos ativos e informações do **CONTRATANTE** por meio de simulações controladas de ataques reais, sendo o ambiente da aplicação do **CONTRATANTE** avaliado em sua totalidade em busca de vulnerabilidades que possam permitir a obtenção de acesso não-autorizado, sendo que a modalidade de teste de intrusão/ penetração a ser realizado será do tipo Black Box;

2.3.2 A **CONTRATADA** deverá realizar testes de intrusão para identificação de vulnerabilidades por meio de simulações de invasão de serviços e infraestrutura (Teste de Invasão) a serem executadas externamente (através da Internet);

2.3.3 A **CONTRATADA** deverá minimamente compreender atividades que busquem encontrar vulnerabilidades em potencial, de eventual má configuração, de falhas em hardwares e softwares desconhecidos, de técnicas de contramedidas ou deficiências na infraestrutura ou sistemas da **CONTRATANTE**;

2.3.4 O **CONTRATANTE** deve criar um usuário interno para a **CONTRATADA** no ambiente da **CONTRATANTE** com todas suas ações logadas para documentação e para atestar a integridade do trabalho realizado pela **CONTRATADA**.

2.4 A **CONTRATADA** deverá elaborar "Relatório de Teste de Invasão" para cada teste realizado no período, apresentando todas as informações sobre o mesmo, contemplando no mínimo: objetivos, premissas e escopo do teste; metodologia de análise de vulnerabilidades; descrição das ações realizadas; vulnerabilidades encontradas; categorização e severidade das vulnerabilidades, recomendações e controles de segurança necessários para correção das vulnerabilidades; apresentação das evidências; referências e ferramentas utilizadas.

2.4.1 Pelo período de 30 (trinta) dias, ou seja, durante todo o prazo de execução, este "Relatório de Teste de Invasão" será o insumo para que a equipe técnica da **CONTRATANTE** possa realizar as mitigações necessárias visando sanar as vulnerabilidades o apontadas.

2.4.2 A **CONTRATADA** deverá apresentar o relatório de vulnerabilidades encontradas e mitigadas em reunião por vídeo conferência com a Diretória de Tecnologia - DTI do **CONTRATANTE**, bem como enviá-lo para o e-mail casi@mpba.mp.br, respeitando-se o prazo de execução definido no **dgr – 2.m**

2.5 Todas as fases dos PENTEST poderão ser acompanhadas e supervisionadas a qualquer momento pela equipe técnica do **CONTRATANTE**;

2.5.1 A **CONTRATADA** deverá reportar ao **CONTRATANTE** quaisquer atividades com suspeita de comprometimento de algum ambiente ou ativo;

2.5.2 O teste de penetração (PENTEST) incluirá, no mínimo, as seguintes técnicas de teste:

2.5.2.1 Ping sweep de intervalos de redes;

2.5.2.2 Verificação de portas de hosts de destino;

2.5.2.3 Verificação de vulnerabilidades dos alvos;

2.5.2.4 Penetração em alvos;

2.5.2.5 Manipulação no nível do aplicativo;

2.5.2.6 Engenharia reversa Java / ActiveX do lado do cliente;

2.5.2.7 Ataques de negação de serviço;

2.5.2.8 Verificações / explorações perigosas.

2.5.3 A metodologia adotada pela **CONTRATADA** durante o PENTEST deve incluir, minimamente, quando pertinente, as seguintes vulnerabilidades:

2.5.3.1 Injeção de Código;

Anexo Contrato 111-2021 (0227530) SEI 19.09.02684.0011790/2021-22 / pg. 763

2.5.3.2 Quebra de Autenticação;

2.5.3.3 Exposição de Dados Sensíveis;

2.5.3.4 Entidades Externas de XML;

2.5.3.5 Quebra de Controle de Acesso;

2.5.3.6 Configuração Incorreta de Segurança;

2.5.3.7 Cross-Site Scripiting (XSS);

2.5.3.8 Desserialização Insegura;

2.5.3.9 Utilização de Componentes com Vulnerabilidades Conhecidas;

2.5.3.10 Log e Monitoramento Ineficientes;

2.6 O prazo para execução dos serviços é de 30 (trinta) dias, contados da data da entrega à **CONTRATADA**, da nota de empenho, acompanhada, se for o caso, da autorização de serviços, e do instrumento contratual;

2.6.1 O prazo de execução poderá ser prorrogado por mais 30 (trinta) dias, desde que seja formalmente solicitado pela **CONTRATADA** antes do termo final do prazo de entrega consignado, mediante justificativa e respectiva comprovação de fato superveniente, aceito pela Instituição.

2.7 Os serviços objeto deste contrato deverão ser executados por profissionais que possuam capacitação técnica compatível com as atividades que lhes forem incumbidas, sob inteira responsabilidade da **CONTRATADA**, que deve orientar os mesmos quanto às suas obrigações e afazeres;

2.8 Os serviços contratados deverão ser obrigatoriamente executados fora das dependências da **CONTRATANTE**, simulando o quanto possível um ataque real, conforme modelo Black Box do PENTEST solicitado.

2.9 O recebimento dos serviços prestados ficará sob a responsabilidade de um representante da Diretoria de Tecnologia da Informação do **CONTRATANTE**, em conjunto com o fiscal do contrato - responsável pela habilitação para pagamentos, caso este não seja integrante daquela Diretoria;

2.9.1 A entrega do Relatório de testes é indispensável ao recebimento do objeto deste instrumento, nos termos definidos no **dgr – 2.6**;

2.9.2 O recebimento provisório se dará no prazo de 05 (cinco) dias, contados da entrega do relatório final de testes;

2.9.3 O **CONTRATANTE** rejeitará, no todo ou em parte, o objeto contratual em desacordo com as condições pactuadas, podendo, entretanto, se lhe convier, decidir pelo recebimento, neste caso com as deduções cabíveis;

2.10 O recebimento definitivo do objeto deste contrato se dará no prazo de 10 (dez) dias, contados da entrega do relatório final de testes, e será concretizado depois de adotados, pelo **CONTRATANTE**, todos os procedimentos contidos nos Ato Normativos internos relativos ao tema, respeitadas as exigências contidas do art. 161 da Lei Estadual- BA nº 9.433/2005;

2.11 O aceite ou aprovação do objeto pelo **CONTRATANTE** não exclui a responsabilidade da **CONTRATADA** por vícios, defeitos ou disparidades com as especificações estabelecidas neste Contrato e no processo de Licitação que o originou, verificadas posteriormente, garantindo-se ao **CONTRATANTE**, inclusive, as faculdades previstas na Lei Federal nº 8.078/90 – Código de Defesa do Consumidor.

CLpUSULA TERCEIRA 1DA DOTAÇÃO ORÇAMENTpRIA

As despesas para o pagamento deste contrato correrão por conta da Dotação Orçamentária a seguir especificada:

C4edhc Uldever O-óv– rlgç-dv/Gr agc-v	Aóác ãP/A/ OE(	Rrndác	Dragdvóác er Rri)-aca ãFclgr(	Nvg)-ruv ev Drasrav
40.601/0003	2002	9900	0100	33.90.40

CLpUSULA QUARTA 1DO PREÇO

4.1 Dá-se ao presente Contrato o valor global de R$ 8.202,67 (oito mil, duzentos e dois reais e sessenta e sete centavos);

4.2 Nos preços computados neste Contrato estão inclusos todos e quaisquer custos necessários ao fiel cumprimento deste instrumento, inclusive todos aqueles relativos a remunerações, encargos sociais, previdenciários e trabalhistas de todo o pessoal disponibilizado pela **CONTRATADA** para a execução do objeto, materiais empregados, aluguéis, licenças, administração, tributos e emolumentos.

Anexo Contrato 111-2021 (0227530) SEI 19.09.02684.0011790/2021-22 / pg. 765

CLpUSULA QUINTA J DOS ACRÉSCIMOS E DAS SUPRESSz ES

5.1 A **CONTRATADA** se obriga a aceitar, quando solicitado e devidamente motivado pela Administração, nas mesmas condições estabelecidas neste instrumento, os acréscimos ou supressões de até 25% (vinte e cinco por cento) do valor inicial atualizado do contrato, na forma da Lei Estadual - BA nº 9.433/2005;

5.2 As supressões poderão ser superiores a 25% (vinte e cinco por cento), desde que haja resultado de acordo entre os contratantes.

CLpUSULA SEXTA 1 DAS CONDIÇz ES DO PAGAMENTO E DA RETENÇÃO DOS TRIBUTOS

6.1 O pagamento dos serviços objeto deste instrumento será processado em parcela única, após a realização dos serviços, mediante apresentação, pela **CONTRATADA**, de Nota Fiscal e demais documentos/certidões cabíveis, documentação que deverá estar devidamente acompanhada do **TERMO DE ACEITE** do objeto pelo **CONTRATANTEÕ**

6.1.1 O pagamento se concluirá no prazo de 08 (oito) dias úteis a contar da data de apresentação da documentação (com respectivo aceite), desde que não haja pendência a ser regularizada;

6.1.2 Verificando-se qualquer pendência impeditiva do pagamento, será considerada como data de apresentação da documentação aquela na qual foi realizada a respectiva regularização;

6.2 As notas fiscais/faturas far-se-ão acompanhar da documentação probatória relativa ao recolhimento dos tributos, que tenham como fato gerador o objeto consignado na **CLpUSULA PRIMEIRA**;

6.3 O **CONTRATANTE** realizará a retenção de impostos ou outras obrigações de natureza tributária, na hipótese de figurar como substituto tributário, de acordo com a legislação vigente;

6.4 Os pagamentos serão efetuados através de ordem bancária, para crédito em conta corrente e agência indicadas pela **CONTRATADA**, preferencialmente em banco de movimentação oficial de recursos do Estado da Bahia;

6.5 A atualização monetária dos pagamentos devidos pelo **CONTRATANTE**, em caso de mora, será calculada considerando a data do vencimento da obrigação e do seu efetivo pagamento, de acordo com a variação do INPC do IBGE *pro rata tempore,* observado, sempre, o disposto no item 6.1 e

seus subitens.

6.5.1 Para efeito de caracterização de mora imputável ao **CONTRATANTE**, não serão considerados eventuais atrasos de pagamento no período de fechamento do exercício financeiro do Estado da Bahia, compreendido entre o final do mês de dezembro e o mês de janeiro do exercício subsequente, decorrentes de circunstâncias alheias à vontade das partes, isto é, por força de bloqueio de rotinas no sistema estadual obrigatoriamente utilizado para a execução dos pagamentos devidos pelo **CONTRATANTE**.

CLpUSULA SÉTIMA J DO REAÁUSTAMENTO E DA REVISÃO DE PREÇOS

7.1 O preço definido na **CLpUSULA QUARTA** é irreajustável;

7.2 A revisão de preços nos termos do inc. XXVI do art. 8º da Lei Estadual nº. 9.433/2005, por interesse da **CONTRATADA**, dependerá de requerimento formal, instruído com a documentação que comprove o desequilíbrio econômico-financeiro do Contrato. Deverá ser instaurada pelo **CONTRATANTE**, entretanto, quando este pretender recompor o preço que se tornou excessivo.

7.2.1 A revisão de preços, se ocorrer, deverá ser formalizada através de celebração de Aditivo Contratual.

CLpUSULA OITAVA J DA VIG; NCIA

O prazo de vigência do presente Contrato será de 90 (noventa) dias, contados da data da sua publicidade no Diário de Justiça Eletrônico (DJ-e) do Poder Judiciário do Estado da Bahia, podendo ser prorrogado, mediante termo aditivo e após manifestação da autoridade competente.

CLpUSULA NONA J DAS OBRIGAÇz ES DA CONTRATADA

9.0 Além das determinações contidas no procedimento que originou esta contratação – que aqui se consideram literalmente transcritas, bem como daquelas decorrentes de lei, a **CONTRATADA,** obriga-se a:

9.1 Promover a execução contratual de acordo com as especificações técnicas e exigências constantes no presente contrato e no procedimento administrativo que o originou, conforme dias, horários e prazos contratados, não podendo eximir-se da obrigação, ainda que parcialmente, sob a alegação de falhas, defeitos ou falta de rede, sistema, pessoal, peça e/ou material;

Anexo Contrato 111-2021 (0227530) SEI 19.09.02684.0011790/2021-22 / pg. 767

9.2 Manter sob sua exclusiva responsabilidade toda a supervisão e direção da mão de obra necessária para execução completa e eficiente dos serviços objeto deste contrato;

9.3 Prestar diretamente os serviços ora contratados, não os transferindo a outrem, no todo ou em parte, ressalvando-se apenas os casos de cisão, fusão ou incorporação da **CONTRATADA**, desde que não impeçam os compromissos pautados neste instrumento contratual, ficando vedada a subcontratação, ainda que parcial, dos serviços que compõem o objeto deste instrumento;

9.4 Acompanhar e informar sobre as atualizações tecnológicas necessárias para executar os serviços adquiridos, realizando as ações necessárias para a implantação dessas atualizações em comum acordo com o **CONTRATANTE**, até o final do contrato, sem ônus para o **CONTRATANTEÕ**

9.5 Manter durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas para a contratação;

9.6 Responsabilizar-se pelo cumprimento das exigências previstas na legislação profissional específica e pelos encargos fiscais e comerciais resultantes da execução do contrato;

9.7 A eventual retenção de tributos pelo **MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA** não implicará na responsabilização deste, em hipótese alguma, por quaisquer penalidades ou gravames futuros, decorrentes de inadimplemento(s) de tributos pela **CONTRATADA**;

9.8 Emitir notas fiscais/faturas de acordo com a legislação, contendo descrição dos serviços, indicação de quantidades, preços unitários e valor total;

9.9 Arcar, quando da execução do objeto contratual, com todo e qualquer dano ou prejuízo, independentemente da natureza, causado ao **MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA** e/ou a terceiros, ainda que por sua culpa, em consequência de erros, imperícia própria ou de auxiliares que estejam sob sua responsabilidade, bem como ressarcir ao MPBA todos os custos decorrentes de indevida paralisação ou interrupção dos serviços contratados;

9.10 Providenciar e manter atualizadas todas as licenças e alvarás junto às repartições competentes que, porventura, sejam necessários à execução do contrato;

9.11 Não introduzir, seja a que título for, nenhuma modificação na especificação do objeto contratado, sem o consentimento prévio, e por escrito, do **MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA**;

9.12 Atender, nos prazos consignados neste instrumento, às recusas ou determinações, pelo **MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA**, de realização/refazimento de serviços que não estejam sendo ou não tenham sido executados de acordo com as Normas Técnicas e/ou em conformidade com as condições deste contrato ou do procedimento que o originou, providenciando sua correção ou realização, sem ônus para o **MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA**;

9.13 Permitir e oferecer condições para a mais ampla e completa fiscalização durante a vigência deste contrato, fornecendo informações, propiciando o acesso à documentação pertinente e à execução contratual, e atendendo às observações e exigências apresentadas pela fiscalização;

9.14 Comunicar formalmente ao **MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA** qualquer anormalidade que interfira no bom andamento da execução do Contrato;

9.15 Prestar todos os esclarecimentos que forem solicitados pelo **MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA**, durante a vigência deste instrumento;

9.16 Assinar o Termo de Confidencialidade constante do **Al r ˆc I** deste instrumento, no qual se comprometerá a guardar os dados e as informações fornecidas, geradas e/ou de propriedade do **MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA**, de forma confidencial e sigilosa, vedada qualquer forma de divulgação, reprodução e/ou cessão.

CLpUSULA DÉCIMA J DAS OBRIGAÇz ES DO CONTRATANTE

10 O **CONTRATANTE,** além das obrigações contidas neste contrato por determinação legal, obriga-se a:

10.1 Fornecer, no prazo de 10 (dez) dias a contar da data da publicação do contrato, as informações necessárias para que a **CONTRATADA** possa executar plenamente o objeto contratado;

Anexo Contrato 111-2021 (0227530) SEI 19.09.02684.0011790/2021-22 / pg. 769

10.2 Realizar os pagamentos devidos pela execução do contrato, nos termos e condições previstos nas **CLpUSULAS QUARTA r SEXTA**;

10.3 Viabilizar, no que for cabível, as condições de execução dos serviços pela **CONTRATADA**, prestando-lhe todas as informações necessárias;

10.4 Acompanhar e fiscalizar o fiel cumprimento dos prazos e das condições de realização do presente contrato, notificando a **CONTRATADA**, por escrito, sobre imperfeições, falhas ou irregularidades constatadas na execução do objeto, para que sejam adotadas as medidas corretivas necessárias;

10.5 Fornecer à **CONTRATADA**, mediante solicitação, atestado de capacidade técnica, quando o fornecimento do objeto atender satisfatoriamente os prazos de entrega, qualidade e demais condições previstas neste Contrato.

CLpUSULA DÉCIMA PRIMEIRA J DA FISCALIZAÇÃO DO CONTRATO

11.1 Na forma das disposições estabelecidas na Lei Estadual-BA nº 9.433/2005, o **CONTRATANTE** designará servidor(es), **sc- – rdt er Pc-gv-dv rasriífdv sv-v gvWfd-** , para a fiscalização deste contrato, tendo poderes, entre outros, para notificar a **CONTRATADA** sobre as irregularidades ou falhas que porventura venham a ser encontradas na execução deste instrumento;

11.2 Incumbe à fiscalização acompanhar e verificar a perfeita execução do contrato, em todas as suas fases, competindo-lhe, primordialmente:

11.2.1 Acompanhar o cumprimento deste instrumento e determinar as providências necessárias à correção de falhas, irregularidades e/ou defeitos, podendo ainda suspender-lhes a execução, sem prejuízos das sanções contratuais legais;

11.2.2 Transmitir à **CONTRATADA** instruções, e comunicar alterações de prazos, cronogramas de execução e especificações do projeto, quando for o caso;

11.2.3 Promover a verificação do fornecimento efetuado, emitindo a competente habilitação para o recebimento de pagamentos;

Anexo Contrato 111-2021 (0227530) SEI 19.09.02684.0011790/2021-22 / pg. 770

11.2.4 Esclarecer as dúvidas da **CONTRATADA**, solicitando ao setor competente do **CONTRATANTE**, se necessário, parecer de especialistas;

11.3 A fiscalização, pelo **CONTRATANTE**, não desobriga a **CONTRATADA** de sua responsabilidade quanto à perfeita execução do objeto contratual;

11.3.1 A ausência de comunicação, por parte do **CONTRATANTE**, sobre irregularidades ou falhas, não exime a **CONTRATADA** das responsabilidades determinadas neste contrato;

11.4 O **CONTRATANTE** poderá recusar, sustar e/ou determinar a substituição de bens ou refazimento de serviços que não estejam sendo ou não tenham sido fornecidos ou executados de acordo com as Normas Técnicas e/ou em conformidade com as condições deste contrato ou do procedimento licitatório que o originou, ou ainda que atentem contra a segurança de terceiros ou de bens;

11.4.1 Qualquer bem ou serviço considerado não aceitável, no todo ou em parte, deverá ser refeito, reparado ou substituído pela **CONTRATADA**, às suas expensas;

11.4.2 A não aceitação de algum bem ou serviço, no todo ou em parte, não implicará na dilação do prazo de execução, salvo expressa concordância do **CONTRATANTE**;

11.5 Para fins de fiscalização, o **CONTRATANTE** poderá solicitar à **CONTRATADA**, a qualquer tempo, os documentos relacionados com a execução do presente contrato.

CLpUSULA DÉCIMA SEGUNDA 1DAS PENALIDADES

12.1 A **CONTRATADA** sujeitar-se-á às sanções administrativas previstas na Lei Estadual-BA nº. 9.433/2005, as quais poderão vir a ser aplicadas após o prévio e devido processo administrativo, assegurando-lhe, sempre, o contraditório e a ampla defesa.

12.2 - Em caso de inadimplemento parcial ou total de obrigações pela **CONTRATADA**, e não sendo suas justificativas aceitas pelo **CONTRATANTE,** àquela poderão ser aplicadas, observado o disposto no item anterior, as seguintes penalidades:

12.2.1 Multa;

Anexo Contrato 111-2021 (0227530) SEI 19.09.02684.0011790/2021-22 / pg. 771

12.2.2 Suspensão temporária de participação em licitação e impedimento de contratar com a Administração pelo prazo de até 05 (cinco) anos;

12.2.3 Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes desta punição e até que seja promovida sua reabilitação perante a Administração Pública Estadual;

12.2.4 Descredenciamento do sistema de registro cadastral.

12.3 Nas hipóteses de aplicação das sanções previstas nos **dgrla x2.2.2 v x2.2.6**, estas serão impostas à **CONTRATADA** cumulativamente com multa;

12.4 A inexecução contratual, inclusive por atraso injustificado na execução do contrato, sujeitará o **CONTRATADA** à multa de mora, que será que será apurada **sc- df-vóác** e graduada de acordo com a gravidade da infração, obedecidos os seguintes limites máximos:

12.4.1 Para hipótese de inexecução relacionada ao cumprimento de obrigação **s-dids vW**

12.4.1.1 - 10% (dez por cento) sobre o valor da nota de empenho ou do Contrato, em caso de descumprimento total da obrigação;
12.4.1.2 - 0,3% (três décimos por cento) ao dia, até o 30º (trigésimo) dia de atraso, sobre o valor total da parte do fornecimento ou serviço não realizado;

12.4.1.3 - 0,7% (sete décimos por cento) por cada dia de atraso subseqüente ao 30º (trigésimo), sobre o valor da parte do fornecimento ou serviço não realizado;

12.4.2 Para hipótese de inexecução relacionada ao cumprimento de obrigação **vi raa4-dv**, assim consideradas aquelas que coadjuvam com a principal:

12.4.2.1 - 0,2% (dois décimos por cento) ao dia, até o 30º (trigésimo) dia de atraso, sobre o valor do contrato;

12.4.2.2 - 0,6% (seis décimos por cento) por cada dia de atraso subsequente ao 30º (trigésimo), sobre o valor do contrato;

12.4.2.3 - Para cada obrigação acessória descumprida, a aplicação dos percentuais definidos nos **a) bdgrla x2.6.2.x r x2.6.2.2**, estará limitada ao montante global de 10% (dez por cento) do valor do contrato;

12.5 A aplicação de multa à **CONTRATADA** não impede que a Administração rescinda unilateralmente o contrato e aplique as demais sanções previstas na Lei Estadual-BA nº 9.433/2005;

12.6 Quando aplicadas, as multas deverão ser pagas espontaneamente no prazo máximo de 05 (cinco) dias úteis, ou serem deduzidas do pagamento a ser efetuado pelo **CONTRATANTE**, caso este deva ocorrer dentro daquele prazo;

12.6.1 Na hipótese de ausência de adimplemento voluntário e impossibilidade de dedução, as multas poderão ser cobradas judicialmente, a critério do **CONTRATANTE**;

12.7 A aplicação de multas não tem caráter compensatório, e o seu pagamento não eximirá a **CONTRATADA** da responsabilidade por perdas e/ou danos decorrentes das infrações cometidas;

12.8 Os custos correspondentes a danos e/ou prejuízos causados por culpa ou dolo da **CONTRATADA** deverão ser ressarcidos ao **CONTRATANTE** no prazo máximo de 05 (cinco) dias úteis, contados da notificação administrativa, sob pena de, sem prejuízo do ressarcimento, serem considerados como hipótese de inadimplemento contratual, sujeita, portanto, à aplicação das sanções administrativas previstas nesta Cláusula.

CLpUSULA DÉCIMA TERCEIRA J DA RESCISÃO

13.1 A inexecução total ou parcial do Contrato ensejará a sua rescisão, com as consequências contratuais previstas no Capítulo IX, Seção VIII - Da Inexecução e da Rescisão dos Contratos, da Lei Estadual-BA nº 9.433/2005;

13.2 O **CONTRATANTE** poderá rescindir unilateral e administrativamente o presente Contrato, nas hipóteses previstas nos incisos I a XVI, XX e XXI do art. 167 da Lei Estadual-BA nº 9.433/2005;

13.3 Havendo rescisão administrativa do presente contrato, baseada em alguma das hipóteses previstas nos incisos II a XII do art. 167 da Lei Estadual-BA nº 9.433/2005, o **CONTRATANTE** poderá adotar, no que couber, quaisquer das medidas discriminadas no art. 169 do supracitado diploma legal.

Anexo Contrato 111-2021 (0227530) SEI 19.09.02684.0011790/2021-22 / pg. 773

CLpUSULA DÉCIMA QUARTA J DA VINCULAÇÃO AO PROCESSO DE DISPENSA DE LICITAÇÃO

Integram o presente contrato, como se nele estivessem transcritas, as cláusulas e condições estabelecidas no processo de dispensa de Licitação que o originou, referido no preâmbulo deste instrumento, bem como a proposta da **CONTRATADA** apresentada no referido expediente, naquilo que não divirja deste ajuste.

CLpUSULA DÉCIMA QUINTA J DA PUBLICIDADE

O **CONTRATANTE** será responsável pela publicação do resumo deste instrumento no Diário da Justiça Eletrônico (DJ-e) do Poder Judiciário do Estado da Bahia, no prazo de 10 (dez) dias corridos, contados a partir da sua assinatura.

CLpUSULA DÉCIMA SEXTA J DO FORO

Fica eleito o Foro da Cidade do Salvador-Bahia, que prevalecerá sobre qualquer outro, por mais privilegiado que seja, para dirimir quaisquer dúvidas oriundas do presente Contrato.

CLpUSULA DÉCIMA SÉTIMA J DAS DISPOSIÇz ES GERAIS

17.1 O **CONTRATANTE** não responderá por quaisquer compromissos assumidos perante terceiros pela **CONTRATADA**, ou seus prepostos, ainda que vinculados à execução do presente Contrato;

17.2 A inadimplência da **CONTRATADA**, com relação a quaisquer custos, despesas, tributos, exigências ou encargos previstos neste contrato, não transfere ao **CONTRATANTE** a responsabilidade pelo seu pagamento, nem poderá onerar o objeto do contrato.

17.3 Aplicar-se-á a Lei Estadual-BA nº 9.433/2005 para dirimir toda e qualquer questão legal relativa à execução deste contrato, em especial os casos omissos.

17.4 Fica assegurado ao **CONTRATANTE** o direito de alterar unilateralmente o Contrato, mediante justificação expressa, nas hipóteses previstas no inciso I do art. 143, para melhor adequação às finalidades de interesse público, desde que mantido o equilíbrio econômico-financeiro original do contrato e respeitados os demais direitos da **CONTRATADA**.

17.5 Não caracterizam novação eventuais variações do valor contratual resultantes de revisão de preços, de compensações financeiras decorrentes

das condições de pagamento nele previstas ou, ainda, de alterações de valor em razão da aplicação de penalidades.

17.6 Inexistindo disposição específica, as obrigações contratuais devem ser praticadas no prazo de 05 (cinco) dias.

E, por assim estarem justos e acordados, assinam o presente Contrato em 02 (duas) vias, de igual teor e forma, para que produza seus efeitos legais, após a publicação depois de lido e achado conforme.

Salvador, _____ de _____ de 2021.

Md dagé-dc PúbW c ec Eagvec ev Bvhdv
F-rer-d c o rW ngcl SdW rd-v Scv-ra
Superintendente de Gestão Administrativa

Sgrfvl d dRvfvrW Srn)-vl óv r Drfrav S.A.
Mv-dv MvnvW B-rev-dcW
Representante Legal

Anexo Contrato 111-2021 (0227530) SEI 19.09.02684.0011790/2021-22 / pg. 775

APENSO I
TERMO DE COMPROMISSO, SIGILO E CONFIDENCIALIDADE

Os abaixo-assinados, de um lado o **MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA**, CNPJ nº 04.142.491/0001-66, situado na cidade de Salvador, a 5ª Avenida, nº 750, Centro Administrativo da Bahia - CAB, doravante denominada **CONTRATANTE**, e de outro lado a **EMPRESA STEFANINI RAFAEL SEGURANÇA E DEFESA S.A.**, CNPJ nº 24.691.488/0001-09, estabelecida à Avenida Eusebio Matoso, nº 1375, Andar 8, Salas 801 e 802, Butantã, CEP 05423-905, São Paulo/SP, doravante denominada **CONTRATADA**, tem entre si justa e acertada, a celebração do presente **TERMO DE COMPROMISSO, SIGILO E CONFIDENCIALIDADE**, através do qual a **CONTRATADA** aceita não divulgar, salvo com autorização prévia e formal, segredos e informações sensíveis de propriedade do **CONTRATANTE,** e se compromete a praticar procedimentos de segurança da informação, em conformidade com as seguintes cláusulas e condições:

1. A **CONTRATADA** compromete-se a manter em caráter confidencial as informações abaixo mencionadas, mesmo após a eventual rescisão do contrato:

1.1 Política de segurança adotada pelo **CONTRATANTE** e configurações de hardware e software decorrentes;

1.2 Processo de instalação, configuração e customizações de produtos, ferramentas e equipamentos e atendimento aos itens de segurança, constantes do Edital de licitação;

1.3 Processo de implantação no ambiente do **CONTRATANTE**, de mecanismos de criptografia e autenticação utilizados;

1.4 Recomendações e implementações decorrentes do processo de consultoria;

1.5 Quaisquer dados que a **CONTRATADA** venha a ter conhecimento em decorrência da presente contratação, pertinentes a hardware, serviços e sistemas aplicativos do **CONTRATANTE**, cujo conhecimento por terceiros exponha o ambiente a riscos de invasão ou resulte na vulnerabilidade do mesmo.

1.6 Não fazer uso das informações prestadas pela **CONTRATANTE** que não seja em absoluto cumprimento ao contrato em questão.

2. A quebra da confidencialidade ou sigilo de informações obtidas na prestação de serviços ensejará multa, responsabilidade criminal na forma da lei, sem prejuízo de outras providências nas demais esferas. A **CONTRATADA** obriga-se a tomar as providências necessárias para assegurar que as informações confidenciais não sejam divulgadas por seus empregados ou agentes.

3. A **CONTRATADA** deve assegurar que todos os seus colaboradores envolvidos diretamente nas atividades objeto da presente contratação guardarão sigilo sobre as informações que porventura tiverem acesso, e que os mesmos se comprometerão a informar, imediatamente, ao seu superior hierárquico, qualquer violação das regras de sigilo, por parte dele ou de qualquer pessoa, inclusive nos casos de violação não intencional.

4. A **CONTRATADA** deverá seguir a Política de Segurança da Informação definida pelo **CONTRATANTE**.

5. O não cumprimento de quaisquer das cláusulas deste Termo implicará em responsabilização administrativa, civil e criminal, de acordo com a legislação vigente.

Em, _____ de _____ de 2021.

_____

Md dagé-dc PúbW/c ec Eagvec ev Bvhd/
Frederico Welington Silveira Soares
Superintendente
CONTRATANTE

_____

Sgrfvl d dRvfvrWSrn)-vlóv r Drfrav S.A.
Mv-d/ MvnvWB-rev-dcW
Rrs-rarl gvl gr LrnvW
CONTRATADA

MINISTÉRIO PÚBLICO
DO ESTADO DA BAHIA

CONTRATO PARA PRESTAÇÃO DE SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO, QUE ENTRE SI CELEBRAM O MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA E A EMPRESA STEFANINI RAFAEL SEGURANÇA E DEFESA S.A, NA FORMA ABAIXO:

CONTRATO Nº 111/2021 - SGA

O **MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA**, CNPJ n º 04.142.491/0001-66, com sede situada à 5ª Avenida, 750, Centro Administrativo da Bahia - CAB, Salvador - BA, neste ato representado, mediante Ato de Delegação nº 70/2014, pelo Superintendente de Gestão Administrativa **Frederico Welington Silveira Soares**, doravante denominado **CONTRATANTE**, e a **EMPRESA STEFANINI RAFAEL SEGURANÇA E DEFESA S.A.**, CNPJ nº 24.691.488/0001-09, estabelecida à Avenida Eusebio Matoso, nº 1375, Andar 8, Salas 801 e 802, Butantã, CEP 05423-905, São Paulo/SP, representada por sua **representante legal,** Sra. **Maria Magali Bredariol,** inscrito no CPF/MF nº [redacted], doravante denominada **CONTRATADA**, com supedâneo no quanto disposto na Lei Estadual-BA nº 9.433/2005, na Medida Provisória nº 961 de maio de 2020, e, ainda, observado o constante no processo de Dispensa de Licitação nº 004/2021-DTI protocolado sob o nº 19.09.02684.0011790/2021-22, o qual integra este instrumento independentemente de transcrição, **CELEBRAM** o presente Contrato, mediante as cláusulas e condições seguintes:

CLÁUSULA PRIMEIRA - DO OBJETO

1.1 Constitui objeto do presente contrato a prestação de serviços técnicos, na área de tecnologia da informação, para a varredura de vulnerabilidades e testes de intrusão – PENTEST – na aplicação WEB VOTO DIGITAL, no formato Black Box, nos termos e condições do presente instrumento.

CLÁUSULA SEGUNDA – DO REGIME DE EXECUÇÃO, DA ENTREGA E DO RECEBIMENTO

2.1 O regime de execução do contrato é o de Empreitada Indireta por preço global;

2.2 O **CONTRATANTE** convocará a **CONTRATADA** para retirar a nota de empenho no prazo de até 05 (cinco) dias contados da data da notificação, a ser efetivada, preferencialmente, por e-mail;

2.2.1 As comprovações da convocação e da entrega/retirada da nota de empenho poderão ocorrer por quaisquer dos seguintes meios: por meio eletrônico (através de confirmação de recebimento de e-mail), aposição de assinatura (para retirada presencial) ou por Aviso de Recebimento dos correios (quando a entrega for via postal).

MARIA MAGALI [redacted]

Anexo contrato 111/2021 (0230695) SEI 19.09.02684.0011790/2021-22 / pg. 778

2.2.2 A **CONTRATADA** poderá solicitar a prorrogação do prazo para retirada/recebimento da nota de empenho, por igual período ao original, por motivo justo e aceito pela Administração, nos termos do art. 124, § 4º, da Lei Estadual – BA nº 9433/2005.

2.3 O Teste de Intrusão/Penetração (PENTEST) compreende o teste de Invasão externa e tem como objetivo principal identificar, possíveis vulnerabilidades na aplicação WEB VOTO DIGITAL da **CONTRATANTE**, observando-se ainda:

2.3.1 Os serviços objeto deste instrumento envolvem o uso de técnicas e ferramentas para tentar o acesso privilegiado aos ativos e informações do **CONTRATANTE** por meio de simulações controladas de ataques reais, sendo o ambiente da aplicação do **CONTRATANTE** avaliado em sua totalidade em busca de vulnerabilidades que possam permitir a obtenção de acesso não-autorizado, sendo que a modalidade de teste de intrusão/penetração a ser realizado será do tipo Black Box;

2.3.2 A **CONTRATADA** deverá realizar testes de intrusão para identificação de vulnerabilidades por meio de simulações de invasão de serviços e infraestrutura (Teste de Invasão) a serem executadas externamente (através da Internet);

2.3.3 A **CONTRATADA** deverá minimamente compreender atividades que busquem encontrar vulnerabilidades em potencial, de eventual má configuração, de falhas em hardwares e softwares desconhecidos, de técnicas de contramedidas ou deficiências na infraestrutura ou sistemas da **CONTRATANTE**;

2.3.4 O **CONTRATANTE** deve criar um usuário interno para a **CONTRATADA** no ambiente da **CONTRATANTE** com todas suas ações logadas para documentação e para atestar a integridade do trabalho realizado pela **CONTRATADA**.

2.4 A **CONTRATADA** deverá elaborar "Relatório de Teste de Invasão" para cada teste realizado no período, apresentando todas as informações sobre o mesmo, contemplando no mínimo: objetivos, premissas e escopo do teste; metodologia de análise de vulnerabilidades; descrição das ações realizadas; vulnerabilidades encontradas; categorização e severidade das vulnerabilidades, recomendações e controles de segurança necessários para correção das vulnerabilidades; apresentação das evidências; referências e ferramentas utilizadas.

2.4.1 Pelo período de 30 (trinta) dias, ou seja, durante todo o prazo de execução, este "Relatório de Teste de Invasão" será o insumo para que a equipe técnica da **CONTRATANTE** possa realizar as mitigações necessárias visando sanar as vulnerabilidades o apontadas.

2.4.2 A **CONTRATADA** deverá apresentar o relatório de vulnerabilidades encontradas e mitigadas em reunião por vídeo conferência com a Diretória de Tecnologia - DTI do **CONTRATANTE**, bem como enviá-lo para o e-mail casi@mpba.mp.br, respeitando-se o prazo de execução definido no **item 2.6**.

2.5 Todas as fases dos PENTEST poderão ser acompanhadas e supervisionadas a qualquer momento pela equipe técnica do **CONTRATANTE**;

MARIA MAGALI
BREDARIOL [redacted]

Anexo contrato 111/2021 (0230695) SEI 19.09.02684.0011790/2021-22 / pg. 779

2.5.1 A **CONTRATADA** deverá reportar ao **CONTRATANTE** quaisquer atividades com suspeita de comprometimento de algum ambiente ou ativo;

2.5.2 O teste de penetração (PENTEST) incluirá, no mínimo, as seguintes técnicas de teste:

2.5.2.1 Ping sweep de intervalos de redes;

2.5.2.2 Verificação de portas de hosts de destino;

2.5.2.3 Verificação de vulnerabilidades dos alvos;

2.5.2.4 Penetração em alvos;

2.5.2.5 Manipulação no nível do aplicativo;

2.5.2.6 Engenharia reversa Java / ActiveX do lado do cliente;

2.5.2.7 Ataques de negação de serviço;

2.5.2.8 Verificações / explorações perigosas.

2.5.3 A metodologia adotada pela **CONTRATADA** durante o PENTEST deve incluir, minimamente, quando pertinente, as seguintes vulnerabilidades:

2.5.3.1 Injeção de Código;

2.5.3.2 Quebra de Autenticação;

2.5.3.3 Exposição de Dados Sensíveis;

2.5.3.4 Entidades Externas de XML;

2.5.3.5 Quebra de Controle de Acesso;

2.5.3.6 Configuração Incorreta de Segurança;

2.5.3.7 Cross-Site Scripiting (XSS);

2.5.3.8 Desserialização Insegura;

2.5.3.9 Utilização de Componentes com Vulnerabilidades Conhecidas;

2.5.3.10 Log e Monitoramento Ineficientes;

2.6 O prazo para execução dos serviços é de 30 (trinta) dias, contados da data da entrega à **CONTRATADA**, da nota de empenho, acompanhada, se for o caso, da autorização de serviços, e do instrumento contratual;

MARIA MAGALI [redacted]

2.6.1 O prazo de execução poderá ser prorrogado por mais 30 (trinta) dias, desde que seja formalmente solicitado pela **CONTRATADA** antes do termo final do prazo de entrega consignado, mediante justificativa e respectiva comprovação de fato superveniente, aceito pela Instituição.

2.7 Os serviços objeto deste contrato deverão ser executados por profissionais que possuam capacitação técnica compatível com as atividades que lhes forem incumbidas, sob inteira responsabilidade da **CONTRATADA**, que deve orientar os mesmos quanto às suas obrigações e afazeres;

2.8 Os serviços contratados deverão ser obrigatoriamente executados fora das dependências da **CONTRATANTE**, simulando o quanto possível um ataque real, conforme modelo Black Box do PENTEST solicitado.

2.9 O recebimento dos serviços prestados ficará sob a responsabilidade de um representante da Diretoria de Tecnologia da Informação do **CONTRATANTE**, em conjunto com o fiscal do contrato - responsável pela habilitação para pagamentos, caso este não seja integrante daquela Diretoria;

2.9.1 A entrega do Relatório de testes é indispensável ao recebimento do objeto deste instrumento, nos termos definidos no **item 2.4**;

2.9.2 O recebimento provisório se dará no prazo de 05 (cinco) dias, contados da entrega do relatório final de testes;

2.9.3 O **CONTRATANTE** rejeitará, no todo ou em parte, o objeto contratual em desacordo com as condições pactuadas, podendo, entretanto, se lhe convier, decidir pelo recebimento, neste caso com as deduções cabíveis;

2.10 O recebimento definitivo do objeto deste contrato se dará no prazo de 10 (dez) dias, contados da entrega do relatório final de testes, e será concretizado depois de adotados, pelo **CONTRATANTE**, todos os procedimentos contidos nos Ato Normativos internos relativos ao tema, respeitadas as exigências contidas do art. 161 da Lei Estadual- BA nº 9.433/2005;

2.11 O aceite ou aprovação do objeto pelo **CONTRATANTE** não exclui a responsabilidade da **CONTRATADA** por vícios, defeitos ou disparidades com as especificações estabelecidas neste Contrato e no processo de Licitação que o originou, verificadas posteriormente, garantindo-se ao **CONTRATANTE**, inclusive, as faculdades previstas na Lei Federal nº 8.078/90 – Código de Defesa do Consumidor.

CLÁUSULA TERCEIRA - DA DOTAÇÃO ORÇAMENTÁRIA

As despesas para o pagamento deste contrato correrão por conta da Dotação Orçamentária a seguir especificada:

[redacted]

Anexo contrato 111/2021 (0230695) SEI 19.09.02684.0011790/2021-22 / pg. 781

Código Unidade Orçamentária/Gestora	Ação (P/A/OE)	Região	Destinação de Recursos (Fonte)	Natureza da Despesa
40.601/0003	2002	9900	0100	33.90.40

CLÁUSULA QUARTA - DO PREÇO

4.1 Dá-se ao presente Contrato o valor global de R$ 8.202,67 (oito mil, duzentos e dois reais e sessenta e sete centavos);

4.2 Nos preços computados neste Contrato estão inclusos todos e quaisquer custos necessários ao fiel cumprimento deste instrumento, inclusive todos aqueles relativos a remunerações, encargos sociais, previdenciários e trabalhistas de todo o pessoal disponibilizado pela **CONTRATADA** para a execução do objeto, materiais empregados, aluguéis, licenças, administração, tributos e emolumentos.

CLÁUSULA QUINTA – DOS ACRÉSCIMOS E DAS SUPRESSÕES

5.1 A **CONTRATADA** se obriga a aceitar, quando solicitado e devidamente motivado pela Administração, nas mesmas condições estabelecidas neste instrumento, os acréscimos ou supressões de até 25% (vinte e cinco por cento) do valor inicial atualizado do contrato, na forma da Lei Estadual - BA nº 9.433/2005;

5.2 As supressões poderão ser superiores a 25% (vinte e cinco por cento), desde que haja resultado de acordo entre os contratantes.

CLÁUSULA SEXTA - DAS CONDIÇÕES DO PAGAMENTO E DA RETENÇÃO DOS TRIBUTOS

6.1 O pagamento dos serviços objeto deste instrumento será processado em parcela única, após a realização dos serviços, mediante apresentação, pela **CONTRATADA**, de Nota Fiscal e demais documentos/certidões cabíveis, documentação que deverá estar devidamente acompanhada do **TERMO DE ACEITE** do objeto pelo **CONTRATANTE;**

6.1.1 O pagamento se concluirá no prazo de 08 (oito) dias úteis a contar da data de apresentação da documentação (com respectivo aceite), desde que não haja pendência a ser regularizada;

6.1.2 Verificando-se qualquer pendência impeditiva do pagamento, será considerada como data de apresentação da documentação aquela na qual foi realizada a respectiva regularização;

6.2 As notas fiscais/faturas far-se-ão acompanhar da documentação probatória relativa ao recolhimento dos tributos, que tenham como fato gerador o objeto consignado na **CLÁUSULA PRIMEIRA**;

[redacted]

Anexo contrato 111/2021 (0230695) SEI 19.09.02684.0011790/2021-22 / pg. 782

6.3 O **CONTRATANTE** realizará a retenção de impostos ou outras obrigações de natureza tributária, na hipótese de figurar como substituto tributário, de acordo com a legislação vigente;

6.4 Os pagamentos serão efetuados através de ordem bancária, para crédito em conta corrente e agência indicadas pela **CONTRATADA**, preferencialmente em banco de movimentação oficial de recursos do Estado da Bahia;

6.5 A atualização monetária dos pagamentos devidos pelo **CONTRATANTE**, em caso de mora, será calculada considerando a data do vencimento da obrigação e do seu efetivo pagamento, de acordo com a variação do INPC do IBGE *pro rata tempore,* observado, sempre, o disposto no item 6.1 e seus subitens.

6.5.1 Para efeito de caracterização de mora imputável ao **CONTRATANTE**, não serão considerados eventuais atrasos de pagamento no período de fechamento do exercício financeiro do Estado da Bahia, compreendido entre o final do mês de dezembro e o mês de janeiro do exercício subsequente, decorrentes de circunstâncias alheias à vontade das partes, isto é, por força de bloqueio de rotinas no sistema estadual obrigatoriamente utilizado para a execução dos pagamentos devidos pelo **CONTRATANTE**.

CLÁUSULA SÉTIMA – DO REAJUSTAMENTO E DA REVISÃO DE PREÇOS

7.1 O preço definido na **CLÁUSULA QUARTA** é irreajustável;

7.2 A revisão de preços nos termos do inc. XXVI do art. 8º da Lei Estadual nº. 9.433/2005, por interesse da **CONTRATADA**, dependerá de requerimento formal, instruído com a documentação que comprove o desequilíbrio econômico-financeiro do Contrato. Deverá ser instaurada pelo **CONTRATANTE**, entretanto, quando este pretender recompor o preço que se tornou excessivo.

7.2.1 A revisão de preços, se ocorrer, deverá ser formalizada através de celebração de Aditivo Contratual.

CLÁUSULA OITAVA – DA VIGÊNCIA

O prazo de vigência do presente Contrato será de 90 (noventa) dias, contados da data da sua publicidade no Diário de Justiça Eletrônico (DJ-e) do Poder Judiciário do Estado da Bahia, podendo ser prorrogado, mediante termo aditivo e após manifestação da autoridade competente.

CLÁUSULA NONA – DAS OBRIGAÇÕES DA CONTRATADA

9.0 Além das determinações contidas no procedimento que originou esta contratação – que aqui se consideram literalmente transcritas, bem como daquelas decorrentes de lei, a **CONTRATADA,** obriga-se a:

Assinado de forma digital

Anexo contrato 111/2021 (0230695) SEI 19.09.02684.0011790/2021-22 / pg. 783

9.1 Promover a execução contratual de acordo com as especificações técnicas e exigências constantes no presente contrato e no procedimento administrativo que o originou, conforme dias, horários e prazos contratados, não podendo eximir-se da obrigação, ainda que parcialmente, sob a alegação de falhas, defeitos ou falta de rede, sistema, pessoal, peça e/ou material;

9.2 Manter sob sua exclusiva responsabilidade toda a supervisão e direção da mão de obra necessária para execução completa e eficiente dos serviços objeto deste contrato;

9.3 Prestar diretamente os serviços ora contratados, não os transferindo a outrem, no todo ou em parte, ressalvando-se apenas os casos de cisão, fusão ou incorporação da **CONTRATADA**, desde que não impeçam os compromissos pautados neste instrumento contratual, ficando vedada a subcontratação, ainda que parcial, dos serviços que compõem o objeto deste instrumento;

9.4 Acompanhar e informar sobre as atualizações tecnológicas necessárias para executar os serviços adquiridos, realizando as ações necessárias para a implantação dessas atualizações em comum acordo com o **CONTRATANTE**, até o final do contrato, sem ônus para o **CONTRATANTE;**

9.5 Manter durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas para a contratação;

9.6 Responsabilizar-se pelo cumprimento das exigências previstas na legislação profissional específica e pelos encargos fiscais e comerciais resultantes da execução do contrato;

9.7 A eventual retenção de tributos pelo **MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA** não implicará na responsabilização deste, em hipótese alguma, por quaisquer penalidades ou gravames futuros, decorrentes de inadimplemento(s) de tributos pela **CONTRATADA**;

9.8 Emitir notas fiscais/faturas de acordo com a legislação, contendo descrição dos serviços, indicação de quantidades, preços unitários e valor total;

9.9 Arcar, quando da execução do objeto contratual, com todo e qualquer dano ou prejuízo, independentemente da natureza, causado ao **MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA** e/ou a terceiros, ainda que por sua culpa, em consequência de erros, imperícia própria ou de auxiliares que estejam sob sua responsabilidade, bem como ressarcir ao MPBA todos os custos decorrentes de indevida paralisação ou interrupção dos serviços contratados;

9.10 Providenciar e manter atualizadas todas as licenças e alvarás junto às repartições competentes que, porventura, sejam necessários à execução do contrato;

9.11 Não introduzir, seja a que título for, nenhuma modificação na especificação do objeto contratado, sem o consentimento prévio, e por escrito, do **MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA**;

[redacted]

Anexo contrato 111/2021 (0230695) SEI 19.09.02684.0011790/2021-22 / pg. 784

9.12 Atender, nos prazos consignados neste instrumento, às recusas ou determinações, pelo **MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA**, de realização/refazimento de serviços que não estejam sendo ou não tenham sido executados de acordo com as Normas Técnicas e/ou em conformidade com as condições deste contrato ou do procedimento que o originou, providenciando sua correção ou realização, sem ônus para o **MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA**;

9.13 Permitir e oferecer condições para a mais ampla e completa fiscalização durante a vigência deste contrato, fornecendo informações, propiciando o acesso à documentação pertinente e à execução contratual, e atendendo às observações e exigências apresentadas pela fiscalização;

9.14 Comunicar formalmente ao **MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA** qualquer anormalidade que interfira no bom andamento da execução do Contrato;

9.15 Prestar todos os esclarecimentos que forem solicitados pelo **MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA**, durante a vigência deste instrumento;

9.16 Assinar o Termo de Confidencialidade constante do **Anexo I** deste instrumento, no qual se comprometerá a guardar os dados e as informações fornecidas, geradas e/ou de propriedade do **MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA**, de forma confidencial e sigilosa, vedada qualquer forma de divulgação, reprodução e/ou cessão.

CLÁUSULA DÉCIMA – DAS OBRIGAÇÕES DO CONTRATANTE

10 O **CONTRATANTE,** além das obrigações contidas neste contrato por determinação legal, obriga-se a:

10.1 Fornecer, no prazo de 10 (dez) dias a contar da data da publicação do contrato, as informações necessárias para que a **CONTRATADA** possa executar plenamente o objeto contratado;

10.2 Realizar os pagamentos devidos pela execução do contrato, nos termos e condições previstos nas **CLÁUSULAS QUARTA e SEXTA**;

10.3 Viabilizar, no que for cabível, as condições de execução dos serviços pela **CONTRATADA**, prestando-lhe todas as informações necessárias;

10.4 Acompanhar e fiscalizar o fiel cumprimento dos prazos e das condições de realização do presente contrato, notificando a **CONTRATADA**, por escrito, sobre imperfeições, falhas ou irregularidades constatadas na execução do objeto, para que sejam adotadas as medidas corretivas necessárias;

10.5 Fornecer à **CONTRATADA**, mediante solicitação, atestado de capacidade técnica, quando o fornecimento do objeto atender satisfatoriamente os prazos de entrega, qualidade e demais condições previstas neste Contrato.

CLÁUSULA DÉCIMA PRIMEIRA – DA FISCALIZAÇÃO DO CONTRATO

11.1 Na forma das disposições estabelecidas na Lei Estadual-BA nº 9.433/2005, o **CONTRATANTE** designará servidor(es), **por meio de Portaria específica para tal fim**, para a fiscalização deste contrato, tendo poderes, entre outros, para notificar a **CONTRATADA** sobre as irregularidades ou falhas que porventura venham a ser encontradas na execução deste instrumento;

11.2 Incumbe à fiscalização acompanhar e verificar a perfeita execução do contrato, em todas as suas fases, competindo-lhe, primordialmente:

11.2.1 Acompanhar o cumprimento deste instrumento e determinar as providências necessárias à correção de falhas, irregularidades e/ou defeitos, podendo ainda suspender-lhes a execução, sem prejuízos das sanções contratuais legais;

11.2.2 Transmitir à **CONTRATADA** instruções, e comunicar alterações de prazos, cronogramas de execução e especificações do projeto, quando for o caso;

11.2.3 Promover a verificação do fornecimento efetuado, emitindo a competente habilitação para o recebimento de pagamentos;

11.2.4 Esclarecer as dúvidas da **CONTRATADA**, solicitando ao setor competente do **CONTRATANTE**, se necessário, parecer de especialistas;

11.3 A fiscalização, pelo **CONTRATANTE**, não desobriga a **CONTRATADA** de sua responsabilidade quanto à perfeita execução do objeto contratual;

11.3.1 A ausência de comunicação, por parte do **CONTRATANTE**, sobre irregularidades ou falhas, não exime a **CONTRATADA** das responsabilidades determinadas neste contrato;

11.4 O **CONTRATANTE** poderá recusar, sustar e/ou determinar a substituição de bens ou refazimento de serviços que não estejam sendo ou não tenham sido fornecidos ou executados de acordo com as Normas Técnicas e/ou em conformidade com as condições deste contrato ou do procedimento licitatório que o originou, ou ainda que atentem contra a segurança de terceiros ou de bens;

11.4.1 Qualquer bem ou serviço considerado não aceitável, no todo ou em parte, deverá ser refeito, reparado ou substituído pela **CONTRATADA**, às suas expensas;

11.4.2 A não aceitação de algum bem ou serviço, no todo ou em parte, não implicará na dilação do prazo de execução, salvo expressa concordância do **CONTRATANTE**;

11.5 Para fins de fiscalização, o **CONTRATANTE** poderá solicitar à **CONTRATADA**, a qualquer tempo, os documentos relacionados com a execução do presente contrato.

CLÁUSULA DÉCIMA SEGUNDA - DAS PENALIDADES

Assinado de forma digital
M
B
[redacted]

Anexo contrato 111/2021 (0230695) SEI 19.09.02684.0011790/2021-22 / pg. 786

12.1 A **CONTRATADA** sujeitar-se-á às sanções administrativas previstas na Lei Estadual-BA nº. 9.433/2005, as quais poderão vir a ser aplicadas após o prévio e devido processo administrativo, assegurando-lhe, sempre, o contraditório e a ampla defesa.

12.2 - Em caso de inadimplemento parcial ou total de obrigações pela **CONTRATADA**, e não sendo suas justificativas aceitas pelo **CONTRATANTE,** àquela poderão ser aplicadas, observado o disposto no item anterior, as seguintes penalidades:

12.2.1 Multa;

12.2.2 Suspensão temporária de participação em licitação e impedimento de contratar com a Administração pelo prazo de até 05 (cinco) anos;

12.2.3 Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes desta punição e até que seja promovida sua reabilitação perante a Administração Pública Estadual;

12.2.4 Descredenciamento do sistema de registro cadastral.

12.3 Nas hipóteses de aplicação das sanções previstas nos **itens 12.2.2 a 12.2.4**, estas serão impostas à **CONTRATADA** cumulativamente com multa;

12.4 A inexecução contratual, inclusive por atraso injustificado na execução do contrato, sujeitará o **CONTRATADA** à multa de mora, que será que será apurada **por infração** e graduada de acordo com a gravidade da infração, obedecidos os seguintes limites máximos:

12.4.1 Para hipótese de inexecução relacionada ao cumprimento de obrigação **principal**:

12.4.1.1 - 10% (dez por cento) sobre o valor da nota de empenho ou do Contrato, em caso de descumprimento total da obrigação;
12.4.1.2 - 0,3% (três décimos por cento) ao dia, até o 30º (trigésimo) dia de atraso, sobre o valor total da parte do fornecimento ou serviço não realizado;

12.4.1.3 - 0,7% (sete décimos por cento) por cada dia de atraso subseqüente ao 30º (trigésimo), sobre o valor da parte do fornecimento ou serviço não realizado;

12.4.2 Para hipótese de inexecução relacionada ao cumprimento de obrigação **acessória**, assim consideradas aquelas que coadjuvam com a principal:

12.4.2.1 - 0,2% (dois décimos por cento) ao dia, até o 30º (trigésimo) dia de atraso, sobre o valor do contrato;

12.4.2.2 - 0,6% (seis décimos por cento) por cada dia de atraso subsequente ao 30º (trigésimo), sobre o valor do contrato;

12.4.2.3 - Para cada obrigação acessória descumprida, a aplicação dos percentuais definidos nos **subitens 12.4.2.1 e 12.4.2.2**, estará limitada ao montante global de 10% (dez por cento) do valor do contrato;

MARIA MAGALI [redacted]

Anexo contrato 111/2021 (0230695) SEI 19.09.02684.0011790/2021-22 / pg. 787

12.5 A aplicação de multa à **CONTRATADA** não impede que a Administração rescinda unilateralmente o contrato e aplique as demais sanções previstas na Lei Estadual-BA nº 9.433/2005;

12.6 Quando aplicadas, as multas deverão ser pagas espontaneamente no prazo máximo de 05 (cinco) dias úteis, ou serem deduzidas do pagamento a ser efetuado pelo **CONTRATANTE**, caso este deva ocorrer dentro daquele prazo;

12.6.1 Na hipótese de ausência de adimplemento voluntário e impossibilidade de dedução, as multas poderão ser cobradas judicialmente, a critério do **CONTRATANTE**;

12.7 A aplicação de multas não tem caráter compensatório, e o seu pagamento não eximirá a **CONTRATADA** da responsabilidade por perdas e/ou danos decorrentes das infrações cometidas;

12.8 Os custos correspondentes a danos e/ou prejuízos causados por culpa ou dolo da **CONTRATADA** deverão ser ressarcidos ao **CONTRATANTE** no prazo máximo de 05 (cinco) dias úteis, contados da notificação administrativa, sob pena de, sem prejuízo do ressarcimento, serem considerados como hipótese de inadimplemento contratual, sujeita, portanto, à aplicação das sanções administrativas previstas nesta Cláusula.

CLÁUSULA DÉCIMA TERCEIRA – DA RESCISÃO

13.1 A inexecução total ou parcial do Contrato ensejará a sua rescisão, com as consequências contratuais previstas no Capítulo IX, Seção VIII - Da Inexecução e da Rescisão dos Contratos, da Lei Estadual-BA nº 9.433/2005;

13.2 O **CONTRATANTE** poderá rescindir unilateral e administrativamente o presente Contrato, nas hipóteses previstas nos incisos I a XVI, XX e XXI do art. 167 da Lei Estadual-BA nº 9.433/2005;

13.3 Havendo rescisão administrativa do presente contrato, baseada em alguma das hipóteses previstas nos incisos II a XII do art. 167 da Lei Estadual-BA nº 9.433/2005, o **CONTRATANTE** poderá adotar, no que couber, quaisquer das medidas discriminadas no art. 169 do supracitado diploma legal.

CLÁUSULA DÉCIMA QUARTA – DA VINCULAÇÃO AO PROCESSO DE DISPENSA DE LICITAÇÃO

Integram o presente contrato, como se nele estivessem transcritas, as cláusulas e condições estabelecidas no processo de dispensa de Licitação que o originou, referido no preâmbulo deste instrumento, bem como a proposta da **CONTRATADA** apresentada no referido expediente, naquilo que não divirja deste ajuste.

CLÁUSULA DÉCIMA QUINTA – DA PUBLICIDADE

[redacted]

Anexo contrato 111/2021 (0230695) SEI 19.09.02684.0011790/2021-22 / pg. 788

O **CONTRATANTE** será responsável pela publicação do resumo deste instrumento no Diário da Justiça Eletrônico (DJ-e) do Poder Judiciário do Estado da Bahia, no prazo de 10 (dez) dias corridos, contados a partir da sua assinatura.

CLÁUSULA DÉCIMA SEXTA – DO FORO

Fica eleito o Foro da Cidade do Salvador-Bahia, que prevalecerá sobre qualquer outro, por mais privilegiado que seja, para dirimir quaisquer dúvidas oriundas do presente Contrato.

CLÁUSULA DÉCIMA SÉTIMA – DAS DISPOSIÇÕES GERAIS

17.1 O **CONTRATANTE** não responderá por quaisquer compromissos assumidos perante terceiros pela **CONTRATADA**, ou seus prepostos, ainda que vinculados à execução do presente Contrato;

17.2 A inadimplência da **CONTRATADA**, com relação a quaisquer custos, despesas, tributos, exigências ou encargos previstos neste contrato, não transfere ao **CONTRATANTE** a responsabilidade pelo seu pagamento, nem poderá onerar o objeto do contrato.

17.3 Aplicar-se-á a Lei Estadual-BA nº 9.433/2005 para dirimir toda e qualquer questão legal relativa à execução deste contrato, em especial os casos omissos.

17.4 Fica assegurado ao **CONTRATANTE** o direito de alterar unilateralmente o Contrato, mediante justificação expressa, nas hipóteses previstas no inciso I do art. 143, para melhor adequação às finalidades de interesse público, desde que mantido o equilíbrio econômico-financeiro original do contrato e respeitados os demais direitos da **CONTRATADA**.

17.5 Não caracterizam novação eventuais variações do valor contratual resultantes de revisão de preços, de compensações financeiras decorrentes das condições de pagamento nele previstas ou, ainda, de alterações de valor em razão da aplicação de penalidades.

17.6 Inexistindo disposição específica, as obrigações contratuais devem ser praticadas no prazo de 05 (cinco) dias.

E, por assim estarem justos e acordados, assinam o presente Contrato em 02 (duas) vias, de igual teor e forma, para que produza seus efeitos legais, após a publicação depois de lido e achado conforme.

Salvador, 05 de novembro de 2021.

MARIA MAGALI BREDARIOL [redacted]

Ministério Público do Estado da Bahia	**Stefanini Rafael Segurança e Defesa S.A.**
Frederico Welington Silveira Soares	**Maria Magali Bredariol**
Superintendente de Gestão Administrativa	Representante Legal

Anexo contrato 111/2021 (0230695) SEI 19.09.02684.0011790/2021-22 / pg. 789

MARIA MAGALI

Anexo contrato 111/2021 (0230695) SEI 19.09.02684.0011790/2021-22 / pg. 790

MINISTÉRIO PÚBLICO
DO ESTADO DA BAHIA

APENSO I
TERMO DE COMPROMISSO, SIGILO E CONFIDENCIALIDADE

Os abaixo-assinados, de um lado o **MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA**, CNPJ nº 04.142.491/0001-66, situado na cidade de Salvador, a 5ª Avenida, nº 750, Centro Administrativo da Bahia - CAB, doravante denominada **CONTRATANTE**, e de outro lado a **EMPRESA STEFANINI RAFAEL SEGURANÇA E DEFESA S.A.**, CNPJ nº 24.691.488/0001-09, estabelecida à Avenida Eusebio Matoso, nº 1375, Andar 8, Salas 801 e 802, Butantã, CEP 05423-905, São Paulo/SP, doravante denominada **CONTRATADA**, tem entre si justa e acertada, a celebração do presente **TERMO DE COMPROMISSO, SIGILO E CONFIDENCIALIDADE**, através do qual a **CONTRATADA** aceita não divulgar, salvo com autorização prévia e formal, segredos e informações sensíveis de propriedade do **CONTRATANTE,** e se compromete a praticar procedimentos de segurança da informação, em conformidade com as seguintes cláusulas e condições:

1. A **CONTRATADA** compromete-se a manter em caráter confidencial as informações abaixo mencionadas, mesmo após a eventual rescisão do contrato:

1.1 Política de segurança adotada pelo **CONTRATANTE** e configurações de hardware e software decorrentes;

1.2 Processo de instalação, configuração e customizações de produtos, ferramentas e equipamentos e atendimento aos itens de segurança, constantes do Edital de licitação;
1.3 Processo de implantação no ambiente do **CONTRATANTE**, de mecanismos de criptografia e autenticação utilizados;

1.4 Recomendações e implementações decorrentes do processo de consultoria;

1.5 Quaisquer dados que a **CONTRATADA** venha a ter conhecimento em decorrência da presente contratação, pertinentes a hardware, serviços e sistemas aplicativos do **CONTRATANTE**, cujo conhecimento por terceiros exponha o ambiente a riscos de invasão ou resulte na vulnerabilidade do mesmo.

1.6 Não fazer uso das informações prestadas pela **CONTRATANTE** que não seja em absoluto cumprimento ao contrato em questão.

2. A quebra da confidencialidade ou sigilo de informações obtidas na prestação de serviços ensejará multa, responsabilidade criminal na forma da lei, sem prejuízo de outras providências nas demais esferas. A **CONTRATADA** obriga-se a tomar as providências necessárias para assegurar que as informações confidenciais não sejam divulgadas por seus empregados ou agentes.

3. A **CONTRATADA** deve assegurar que todos os seus colaboradores envolvidos diretamente nas atividades objeto da presente contratação guardarão sigilo sobre as informações que porventura tiverem acesso, e que os mesmos se comprometerão a informar, imediatamente, ao seu superior hierárquico, qualquer violação das regras de sigilo, por parte dele ou de qualquer pessoa, inclusive nos casos de violação não intencional.

[redacted]

4. A **CONTRATADA** deverá seguir a Política de Segurança da Informação definida pelo **CONTRATANTE**.

5. O não cumprimento de quaisquer das cláusulas deste Termo implicará em responsabilização administrativa, civil e criminal, de acordo com a legislação vigente.

Em, 05 de novembro de 2021.

Ministério Público do Estado da Bahia
Frederico Welington Silveira Soares
Superintendente

C[redacted]

Stefanini Rafael Segurança e Defesa S.A.
Maria Magali Bredariol
Representante Legal
CONTRATADA

MINISTÉRIO PÚBLICO
DO ESTADO DA BAHIA

DESPACHO

Prezados ,

Segue contrato 111/2021 assinado para coleta de assinatura da Superintendencia.

Documento assinado eletronicamente por **Fabiana Costa do Nascimento** em 02/88/1018, às 8: f1. , conºorme artI 8", ⱡbb, L4L, da 9ei 88I. 86/100: I

A autenticidade do documento pode ser conºerida no site https//seiIsistemasImp4aImpI4r/sei/controlador_externoIphp?acao=documento_conºerir&id_orgao_acesso_externo=0 inºormando o código veriºicador **0230719** e o código CRC **913B911C**I

MINISTÉRIO PÚBLICO
DO ESTADO DA BAHIA

DESPACHO

Retorne-se o presente expediente à DCCL/Coordenação de Elaboração e Acompanhamento de Contratos, Convênios e Licitações com o contrato devidamente assinado.

Documento assinado eletronicamente por **Frederico Welington Silveira Soares** em 03/00/13102, s 0à:352conforme art. 0º2III2"b"2da Lei 00.409/1336.

A autenticidade do documento pode ser conferida no site https://sei.sistemas.mpba.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=3 informando o código verificador **0230765** e o código CRC **AE034011**.

MINISTÉRIO PÚBLICO
DO ESTADO DA BAHIA

CONTRATO PARA PRESTAÇÃO DE SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO, QUE ENTRE SI CELEBRAM O MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA E A EMPRESA STEFANINI RAFAEL SEGURANÇA E DEFESA S.A, NA FORMA ABAIXO:

CONTRATO Nº 111/2021 - SGA

O **MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA**, CNPJ n º 04.142.491/0001-66, com sede situada à 5ª Avenida, 750, Centro Administrativo da Bahia - CAB, Salvador - BA, neste ato representado, mediante Ato de Delegação nº 70/2014, pelo Superintendente de Gestão Administrativa **Frederico Welington Silveira Soares**, doravante denominado **CONTRATANTE**, e a **EMPRESA STEFANINI RAFAEL SEGURANÇA E DEFESA S.A.**, CNPJ nº 24.691.488/0001-09, estabelecida à Avenida Eusebio Matoso, nº 1375, Andar 8, Salas 801 e 802, Butantã, CEP 05423-905, São Paulo/SP, representada por sua **representante legal,** Sra. **Maria Magali Bredariol,** inscrito no CPF/MF nº [redacted] doravante denominada **CONTRATADA**, com supedâneo no quanto disposto na Lei Estadual-BA nº 9.433/2005, na Medida Provisória nº 961 de maio de 2020, e, ainda, observado o constante no processo de Dispensa de Licitação nº 004/2021-DTI protocolado sob o nº 19.09.02684.0011790/2021-22, o qual integra este instrumento independentemente de transcrição, **CELEBRAM** o presente Contrato, mediante as cláusulas e condições seguintes:

CLÁUSULA PRIMEIRA - DO OBJETO

1.1 Constitui objeto do presente contrato a prestação de serviços técnicos, na área de tecnologia da informação, para a varredura de vulnerabilidades e testes de intrusão – PENTEST – na aplicação WEB VOTO DIGITAL, no formato Black Box, nos termos e condições do presente instrumento.

CLÁUSULA SEGUNDA – DO REGIME DE EXECUÇÃO, DA ENTREGA E DO RECEBIMENTO

2.1 O regime de execução do contrato é o de Empreitada Indireta por preço global;

2.2 O **CONTRATANTE** convocará a **CONTRATADA** para retirar a nota de empenho no prazo de até 05 (cinco) dias contados da data da notificação, a ser efetivada, preferencialmente, por e-mail;

2.2.1 As comprovações da convocação e da entrega/retirada da nota de empenho poderão ocorrer por quaisquer dos seguintes meios: por meio eletrônico (através de confirmação de recebimento de e-mail), aposição de assinatura (para retirada presencial) ou por Aviso de Recebimento dos correios (quando a entrega for via postal).

[redacted] [redacted]

Anexo Contrato assinado SGA (0232606) SEI 19.09.02684.0011790/2021-22 / pg. 795

2.2.2 A **CONTRATADA** poderá solicitar a prorrogação do prazo para retirada/recebimento da nota de empenho, por igual período ao original, por motivo justo e aceito pela Administração, nos termos do art. 124, § 4º, da Lei Estadual – BA nº 9433/2005.

2.3 O Teste de Intrusão/Penetração (PENTEST) compreende o teste de Invasão externa e tem como objetivo principal identificar, possíveis vulnerabilidades na aplicação WEB VOTO DIGITAL da **CONTRATANTE**, observando-se ainda:

2.3.1 Os serviços objeto deste instrumento envolvem o uso de técnicas e ferramentas para tentar o acesso privilegiado aos ativos e informações do **CONTRATANTE** por meio de simulações controladas de ataques reais, sendo o ambiente da aplicação do **CONTRATANTE** avaliado em sua totalidade em busca de vulnerabilidades que possam permitir a obtenção de acesso não-autorizado, sendo que a modalidade de teste de intrusão/penetração a ser realizado será do tipo Black Box;

2.3.2 A **CONTRATADA** deverá realizar testes de intrusão para identificação de vulnerabilidades por meio de simulações de invasão de serviços e infraestrutura (Teste de Invasão) a serem executadas externamente (através da Internet);

2.3.3 A **CONTRATADA** deverá minimamente compreender atividades que busquem encontrar vulnerabilidades em potencial, de eventual má configuração, de falhas em hardwares e softwares desconhecidos, de técnicas de contramedidas ou deficiências na infraestrutura ou sistemas da **CONTRATANTE**;

2.3.4 O **CONTRATANTE** deve criar um usuário interno para a **CONTRATADA** no ambiente da **CONTRATANTE** com todas suas ações logadas para documentação e para atestar a integridade do trabalho realizado pela **CONTRATADA**.

2.4 A **CONTRATADA** deverá elaborar "Relatório de Teste de Invasão" para cada teste realizado no período, apresentando todas as informações sobre o mesmo, contemplando no mínimo: objetivos, premissas e escopo do teste; metodologia de análise de vulnerabilidades; descrição das ações realizadas; vulnerabilidades encontradas; categorização e severidade das vulnerabilidades, recomendações e controles de segurança necessários para correção das vulnerabilidades; apresentação das evidências; referências e ferramentas utilizadas.

2.4.1 Pelo período de 30 (trinta) dias, ou seja, durante todo o prazo de execução, este "Relatório de Teste de Invasão" será o insumo para que a equipe técnica da **CONTRATANTE** possa realizar as mitigações necessárias visando sanar as vulnerabilidades o apontadas.

2.4.2 A **CONTRATADA** deverá apresentar o relatório de vulnerabilidades encontradas e mitigadas em reunião por vídeo conferência com a Diretória de Tecnologia - DTI do **CONTRATANTE**, bem como enviá-lo para o e-mail casi@mpba.mp.br, respeitando-se o prazo de execução definido no **item 2.6**.

2.5 Todas as fases dos PENTEST poderão ser acompanhadas e supervisionadas a qualquer momento pela equipe técnica do **CONTRATANTE**;

FREDERICO [redacted]

[redacted]

Anexo Contrato assinado SGA (0232606) SEI 19.09.02684.0011790/2021-22 / pg. 796

2.5.1 A **CONTRATADA** deverá reportar ao **CONTRATANTE** quaisquer atividades com suspeita de comprometimento de algum ambiente ou ativo;

2.5.2 O teste de penetração (PENTEST) incluirá, no mínimo, as seguintes técnicas de teste:

2.5.2.1 Ping sweep de intervalos de redes;

2.5.2.2 Verificação de portas de hosts de destino;

2.5.2.3 Verificação de vulnerabilidades dos alvos;

2.5.2.4 Penetração em alvos;

2.5.2.5 Manipulação no nível do aplicativo;

2.5.2.6 Engenharia reversa Java / ActiveX do lado do cliente;

2.5.2.7 Ataques de negação de serviço;

2.5.2.8 Verificações / explorações perigosas.

2.5.3 A metodologia adotada pela **CONTRATADA** durante o PENTEST deve incluir, minimamente, quando pertinente, as seguintes vulnerabilidades:

2.5.3.1 Injeção de Código;

2.5.3.2 Quebra de Autenticação;

2.5.3.3 Exposição de Dados Sensíveis;

2.5.3.4 Entidades Externas de XML;

2.5.3.5 Quebra de Controle de Acesso;

2.5.3.6 Configuração Incorreta de Segurança;

2.5.3.7 Cross-Site Scripiting (XSS);

2.5.3.8 Desserialização Insegura;

2.5.3.9 Utilização de Componentes com Vulnerabilidades Conhecidas;

2.5.3.10 Log e Monitoramento Ineficientes;

2.6 O prazo para execução dos serviços é de 30 (trinta) dias, contados da data da entrega à **CONTRATADA**, da nota de empenho, acompanhada, se for o caso, da autorização de serviços, e do instrumento contratual;

[redacted] [redacted]

Anexo Contrato assinado SGA (0232606) SEI 19.09.02684.0011790/2021-22 / pg. 797

2.6.1 O prazo de execução poderá ser prorrogado por mais 30 (trinta) dias, desde que seja formalmente solicitado pela **CONTRATADA** antes do termo final do prazo de entrega consignado, mediante justificativa e respectiva comprovação de fato superveniente, aceito pela Instituição.

2.7 Os serviços objeto deste contrato deverão ser executados por profissionais que possuam capacitação técnica compatível com as atividades que lhes forem incumbidas, sob inteira responsabilidade da **CONTRATADA**, que deve orientar os mesmos quanto às suas obrigações e afazeres;

2.8 Os serviços contratados deverão ser obrigatoriamente executados fora das dependências da **CONTRATANTE**, simulando o quanto possível um ataque real, conforme modelo Black Box do PENTEST solicitado.

2.9 O recebimento dos serviços prestados ficará sob a responsabilidade de um representante da Diretoria de Tecnologia da Informação do **CONTRATANTE**, em conjunto com o fiscal do contrato - responsável pela habilitação para pagamentos, caso este não seja integrante daquela Diretoria;

2.9.1 A entrega do Relatório de testes é indispensável ao recebimento do objeto deste instrumento, nos termos definidos no **item 2.4**;

2.9.2 O recebimento provisório se dará no prazo de 05 (cinco) dias, contados da entrega do relatório final de testes;

2.9.3 O **CONTRATANTE** rejeitará, no todo ou em parte, o objeto contratual em desacordo com as condições pactuadas, podendo, entretanto, se lhe convier, decidir pelo recebimento, neste caso com as deduções cabíveis;

2.10 O recebimento definitivo do objeto deste contrato se dará no prazo de 10 (dez) dias, contados da entrega do relatório final de testes, e será concretizado depois de adotados, pelo **CONTRATANTE**, todos os procedimentos contidos nos Ato Normativos internos relativos ao tema, respeitadas as exigências contidas do art. 161 da Lei Estadual- BA nº 9.433/2005;

2.11 O aceite ou aprovação do objeto pelo **CONTRATANTE** não exclui a responsabilidade da **CONTRATADA** por vícios, defeitos ou disparidades com as especificações estabelecidas neste Contrato e no processo de Licitação que o originou, verificadas posteriormente, garantindo-se ao **CONTRATANTE**, inclusive, as faculdades previstas na Lei Federal nº 8.078/90 – Código de Defesa do Consumidor.

CLÁUSULA TERCEIRA - DA DOTAÇÃO ORÇAMENTÁRIA

As despesas para o pagamento deste contrato correrão por conta da Dotação Orçamentária a seguir especificada:

Assinado de forma digital por [redacted]

[redacted]

Anexo Contrato assinado SGA (0232606) SEI 19.09.02684.0011790/2021-22 / pg. 798

Código Unidade Orçamentária/Gestora	Ação (P/A/OE)	Região	Destinação de Recursos (Fonte)	Natureza da Despesa
40.601/0003	2002	9900	0100	33.90.40

CLÁUSULA QUARTA - DO PREÇO

4.1 Dá-se ao presente Contrato o valor global de R$ 8.202,67 (oito mil, duzentos e dois reais e sessenta e sete centavos);

4.2 Nos preços computados neste Contrato estão inclusos todos e quaisquer custos necessários ao fiel cumprimento deste instrumento, inclusive todos aqueles relativos a remunerações, encargos sociais, previdenciários e trabalhistas de todo o pessoal disponibilizado pela **CONTRATADA** para a execução do objeto, materiais empregados, aluguéis, licenças, administração, tributos e emolumentos.

CLÁUSULA QUINTA – DOS ACRÉSCIMOS E DAS SUPRESSÕES

5.1 A **CONTRATADA** se obriga a aceitar, quando solicitado e devidamente motivado pela Administração, nas mesmas condições estabelecidas neste instrumento, os acréscimos ou supressões de até 25% (vinte e cinco por cento) do valor inicial atualizado do contrato, na forma da Lei Estadual - BA nº 9.433/2005;

5.2 As supressões poderão ser superiores a 25% (vinte e cinco por cento), desde que haja resultado de acordo entre os contratantes.

CLÁUSULA SEXTA - DAS CONDIÇÕES DO PAGAMENTO E DA RETENÇÃO DOS TRIBUTOS

6.1 O pagamento dos serviços objeto deste instrumento será processado em parcela única, após a realização dos serviços, mediante apresentação, pela **CONTRATADA**, de Nota Fiscal e demais documentos/certidões cabíveis, documentação que deverá estar devidamente acompanhada do **TERMO DE ACEITE** do objeto pelo **CONTRATANTE;**

6.1.1 O pagamento se concluirá no prazo de 08 (oito) dias úteis a contar da data de apresentação da documentação (com respectivo aceite), desde que não haja pendência a ser regularizada;

6.1.2 Verificando-se qualquer pendência impeditiva do pagamento, será considerada como data de apresentação da documentação aquela na qual foi realizada a respectiva regularização;

6.2 As notas fiscais/faturas far-se-ão acompanhar da documentação probatória relativa ao recolhimento dos tributos, que tenham como fato gerador o objeto consignado na **CLÁUSULA PRIMEIRA**;

[redacted]

MARIA MAGALI [redacted]

Anexo Contrato assinado SGA (0232606) SEI 19.09.02684.0011790/2021-22 / pg. 799

6.3 O **CONTRATANTE** realizará a retenção de impostos ou outras obrigações de natureza tributária, na hipótese de figurar como substituto tributário, de acordo com a legislação vigente;

6.4 Os pagamentos serão efetuados através de ordem bancária, para crédito em conta corrente e agência indicadas pela **CONTRATADA**, preferencialmente em banco de movimentação oficial de recursos do Estado da Bahia;

6.5 A atualização monetária dos pagamentos devidos pelo **CONTRATANTE**, em caso de mora, será calculada considerando a data do vencimento da obrigação e do seu efetivo pagamento, de acordo com a variação do INPC do IBGE *pro rata tempore,* observado, sempre, o disposto no item 6.1 e seus subitens.

6.5.1 Para efeito de caracterização de mora imputável ao **CONTRATANTE**, não serão considerados eventuais atrasos de pagamento no período de fechamento do exercício financeiro do Estado da Bahia, compreendido entre o final do mês de dezembro e o mês de janeiro do exercício subsequente, decorrentes de circunstâncias alheias à vontade das partes, isto é, por força de bloqueio de rotinas no sistema estadual obrigatoriamente utilizado para a execução dos pagamentos devidos pelo **CONTRATANTE**.

CLÁUSULA SÉTIMA – DO REAJUSTAMENTO E DA REVISÃO DE PREÇOS

7.1 O preço definido na **CLÁUSULA QUARTA** é irreajustável;

7.2 A revisão de preços nos termos do inc. XXVI do art. 8º da Lei Estadual nº. 9.433/2005, por interesse da **CONTRATADA**, dependerá de requerimento formal, instruído com a documentação que comprove o desequilíbrio econômico-financeiro do Contrato. Deverá ser instaurada pelo **CONTRATANTE**, entretanto, quando este pretender recompor o preço que se tornou excessivo.

7.2.1 A revisão de preços, se ocorrer, deverá ser formalizada através de celebração de Aditivo Contratual.

CLÁUSULA OITAVA – DA VIGÊNCIA

O prazo de vigência do presente Contrato será de 90 (noventa) dias, contados da data da sua publicidade no Diário de Justiça Eletrônico (DJ-e) do Poder Judiciário do Estado da Bahia, podendo ser prorrogado, mediante termo aditivo e após manifestação da autoridade competente.

CLÁUSULA NONA – DAS OBRIGAÇÕES DA CONTRATADA

9.0 Além das determinações contidas no procedimento que originou esta contratação – que aqui se consideram literalmente transcritas, bem como daquelas decorrentes de lei, a **CONTRATADA,** obriga-se a:

FREDERICO Assinado de forma digital por [redacted]

[redacted]

Anexo Contrato assinado SGA (0232606) SEI 19.09.02684.0011790/2021-22 / pg. 800

9.1 Promover a execução contratual de acordo com as especificações técnicas e exigências constantes no presente contrato e no procedimento administrativo que o originou, conforme dias, horários e prazos contratados, não podendo eximir-se da obrigação, ainda que parcialmente, sob a alegação de falhas, defeitos ou falta de rede, sistema, pessoal, peça e/ou material;

9.2 Manter sob sua exclusiva responsabilidade toda a supervisão e direção da mão de obra necessária para execução completa e eficiente dos serviços objeto deste contrato;

9.3 Prestar diretamente os serviços ora contratados, não os transferindo a outrem, no todo ou em parte, ressalvando-se apenas os casos de cisão, fusão ou incorporação da **CONTRATADA**, desde que não impeçam os compromissos pautados neste instrumento contratual, ficando vedada a subcontratação, ainda que parcial, dos serviços que compõem o objeto deste instrumento;

9.4 Acompanhar e informar sobre as atualizações tecnológicas necessárias para executar os serviços adquiridos, realizando as ações necessárias para a implantação dessas atualizações em comum acordo com o **CONTRATANTE**, até o final do contrato, sem ônus para o **CONTRATANTE;**

9.5 Manter durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas para a contratação;

9.6 Responsabilizar-se pelo cumprimento das exigências previstas na legislação profissional específica e pelos encargos fiscais e comerciais resultantes da execução do contrato;

9.7 A eventual retenção de tributos pelo **MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA** não implicará na responsabilização deste, em hipótese alguma, por quaisquer penalidades ou gravames futuros, decorrentes de inadimplemento(s) de tributos pela **CONTRATADA**;

9.8 Emitir notas fiscais/faturas de acordo com a legislação, contendo descrição dos serviços, indicação de quantidades, preços unitários e valor total;

9.9 Arcar, quando da execução do objeto contratual, com todo e qualquer dano ou prejuízo, independentemente da natureza, causado ao **MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA** e/ou a terceiros, ainda que por sua culpa, em consequência de erros, imperícia própria ou de auxiliares que estejam sob sua responsabilidade, bem como ressarcir ao MPBA todos os custos decorrentes de indevida paralisação ou interrupção dos serviços contratados;

9.10 Providenciar e manter atualizadas todas as licenças e alvarás junto às repartições competentes que, porventura, sejam necessários à execução do contrato;

9.11 Não introduzir, seja a que título for, nenhuma modificação na especificação do objeto contratado, sem o consentimento prévio, e por escrito, do **MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA**;

[redacted] [redacted]

Anexo Contrato assinado SGA (0232606) SEI 19.09.02684.0011790/2021-22 / pg. 801

9.12 Atender, nos prazos consignados neste instrumento, às recusas ou determinações, pelo **MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA**, de realização/refazimento de serviços que não estejam sendo ou não tenham sido executados de acordo com as Normas Técnicas e/ou em conformidade com as condições deste contrato ou do procedimento que o originou, providenciando sua correção ou realização, sem ônus para o **MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA**;

9.13 Permitir e oferecer condições para a mais ampla e completa fiscalização durante a vigência deste contrato, fornecendo informações, propiciando o acesso à documentação pertinente e à execução contratual, e atendendo às observações e exigências apresentadas pela fiscalização;

9.14 Comunicar formalmente ao **MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA** qualquer anormalidade que interfira no bom andamento da execução do Contrato;

9.15 Prestar todos os esclarecimentos que forem solicitados pelo **MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA**, durante a vigência deste instrumento;

9.16 Assinar o Termo de Confidencialidade constante do **Anexo I** deste instrumento, no qual se comprometerá a guardar os dados e as informações fornecidas, geradas e/ou de propriedade do **MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA**, de forma confidencial e sigilosa, vedada qualquer forma de divulgação, reprodução e/ou cessão.

CLÁUSULA DÉCIMA – DAS OBRIGAÇÕES DO CONTRATANTE

10 O **CONTRATANTE,** além das obrigações contidas neste contrato por determinação legal, obriga-se a:

10.1 Fornecer, no prazo de 10 (dez) dias a contar da data da publicação do contrato, as informações necessárias para que a **CONTRATADA** possa executar plenamente o objeto contratado;

10.2 Realizar os pagamentos devidos pela execução do contrato, nos termos e condições previstos nas **CLÁUSULAS QUARTA e SEXTA**;

10.3 Viabilizar, no que for cabível, as condições de execução dos serviços pela **CONTRATADA**, prestando-lhe todas as informações necessárias;

10.4 Acompanhar e fiscalizar o fiel cumprimento dos prazos e das condições de realização do presente contrato, notificando a **CONTRATADA**, por escrito, sobre imperfeições, falhas ou irregularidades constatadas na execução do objeto, para que sejam adotadas as medidas corretivas necessárias;

10.5 Fornecer à **CONTRATADA**, mediante solicitação, atestado de capacidade técnica, quando o fornecimento do objeto atender satisfatoriamente os prazos de entrega, qualidade e demais condições previstas neste Contrato.

[redacted]

Anexo Contrato assinado SGA (0232606) SEI 19.09.02684.0011790/2021-22 / pg. 802

CLÁUSULA DÉCIMA PRIMEIRA – DA FISCALIZAÇÃO DO CONTRATO

11.1 Na forma das disposições estabelecidas na Lei Estadual-BA nº 9.433/2005, o **CONTRATANTE** designará servidor(es), **por meio de Portaria específica para tal fim**, para a fiscalização deste contrato, tendo poderes, entre outros, para notificar a **CONTRATADA** sobre as irregularidades ou falhas que porventura venham a ser encontradas na execução deste instrumento;

11.2 Incumbe à fiscalização acompanhar e verificar a perfeita execução do contrato, em todas as suas fases, competindo-lhe, primordialmente:

11.2.1 Acompanhar o cumprimento deste instrumento e determinar as providências necessárias à correção de falhas, irregularidades e/ou defeitos, podendo ainda suspender-lhes a execução, sem prejuízos das sanções contratuais legais;

11.2.2 Transmitir à **CONTRATADA** instruções, e comunicar alterações de prazos, cronogramas de execução e especificações do projeto, quando for o caso;

11.2.3 Promover a verificação do fornecimento efetuado, emitindo a competente habilitação para o recebimento de pagamentos;

11.2.4 Esclarecer as dúvidas da **CONTRATADA**, solicitando ao setor competente do **CONTRATANTE**, se necessário, parecer de especialistas;

11.3 A fiscalização, pelo **CONTRATANTE**, não desobriga a **CONTRATADA** de sua responsabilidade quanto à perfeita execução do objeto contratual;

11.3.1 A ausência de comunicação, por parte do **CONTRATANTE**, sobre irregularidades ou falhas, não exime a **CONTRATADA** das responsabilidades determinadas neste contrato;

11.4 O **CONTRATANTE** poderá recusar, sustar e/ou determinar a substituição de bens ou refazimento de serviços que não estejam sendo ou não tenham sido fornecidos ou executados de acordo com as Normas Técnicas e/ou em conformidade com as condições deste contrato ou do procedimento licitatório que o originou, ou ainda que atentem contra a segurança de terceiros ou de bens;

11.4.1 Qualquer bem ou serviço considerado não aceitável, no todo ou em parte, deverá ser refeito, reparado ou substituído pela **CONTRATADA**, às suas expensas;

11.4.2 A não aceitação de algum bem ou serviço, no todo ou em parte, não implicará na dilação do prazo de execução, salvo expressa concordância do **CONTRATANTE**;

11.5 Para fins de fiscalização, o **CONTRATANTE** poderá solicitar à **CONTRATADA**, a qualquer tempo, os documentos relacionados com a execução do presente contrato.

CLÁUSULA DÉCIMA SEGUNDA - DAS PENALIDADES

FREDERICO [redacted]
13:02:25 -03'00'

[redacted]

Anexo Contrato assinado SGA (0232606) SEI 19.09.02684.0011790/2021-22 / pg. 803

12.1 A **CONTRATADA** sujeitar-se-á às sanções administrativas previstas na Lei Estadual-BA nº. 9.433/2005, as quais poderão vir a ser aplicadas após o prévio e devido processo administrativo, assegurando-lhe, sempre, o contraditório e a ampla defesa.

12.2 - Em caso de inadimplemento parcial ou total de obrigações pela **CONTRATADA**, e não sendo suas justificativas aceitas pelo **CONTRATANTE,** àquela poderão ser aplicadas, observado o disposto no item anterior, as seguintes penalidades:

12.2.1 Multa;

12.2.2 Suspensão temporária de participação em licitação e impedimento de contratar com a Administração pelo prazo de até 05 (cinco) anos;

12.2.3 Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes desta punição e até que seja promovida sua reabilitação perante a Administração Pública Estadual;

12.2.4 Descredenciamento do sistema de registro cadastral.

12.3 Nas hipóteses de aplicação das sanções previstas nos **itens 12.2.2 a 12.2.4**, estas serão impostas à **CONTRATADA** cumulativamente com multa;

12.4 A inexecução contratual, inclusive por atraso injustificado na execução do contrato, sujeitará o **CONTRATADA** à multa de mora, que será que será apurada **por infração** e graduada de acordo com a gravidade da infração, obedecidos os seguintes limites máximos:

12.4.1 Para hipótese de inexecução relacionada ao cumprimento de obrigação **principal**:

12.4.1.1 - 10% (dez por cento) sobre o valor da nota de empenho ou do Contrato, em caso de descumprimento total da obrigação;
12.4.1.2 - 0,3% (três décimos por cento) ao dia, até o 30º (trigésimo) dia de atraso, sobre o valor total da parte do fornecimento ou serviço não realizado;

12.4.1.3 - 0,7% (sete décimos por cento) por cada dia de atraso subseqüente ao 30º (trigésimo), sobre o valor da parte do fornecimento ou serviço não realizado;

12.4.2 Para hipótese de inexecução relacionada ao cumprimento de obrigação **acessória**, assim consideradas aquelas que coadjuvam com a principal:

12.4.2.1 - 0,2% (dois décimos por cento) ao dia, até o 30º (trigésimo) dia de atraso, sobre o valor do contrato;

12.4.2.2 - 0,6% (seis décimos por cento) por cada dia de atraso subsequente ao 30º (trigésimo), sobre o valor do contrato;

12.4.2.3 - Para cada obrigação acessória descumprida, a aplicação dos percentuais definidos nos **subitens 12.4.2.1 e 12.4.2.2**, estará limitada ao montante global de 10% (dez por cento) do valor do contrato;

[redacted] [redacted]

Anexo Contrato assinado SGA (0232606) SEI 19.09.02684.0011790/2021-22 / pg. 804

12.5 A aplicação de multa à **CONTRATADA** não impede que a Administração rescinda unilateralmente o contrato e aplique as demais sanções previstas na Lei Estadual-BA nº 9.433/2005;

12.6 Quando aplicadas, as multas deverão ser pagas espontaneamente no prazo máximo de 05 (cinco) dias úteis, ou serem deduzidas do pagamento a ser efetuado pelo **CONTRATANTE**, caso este deva ocorrer dentro daquele prazo;

12.6.1 Na hipótese de ausência de adimplemento voluntário e impossibilidade de dedução, as multas poderão ser cobradas judicialmente, a critério do **CONTRATANTE**;

12.7 A aplicação de multas não tem caráter compensatório, e o seu pagamento não eximirá a **CONTRATADA** da responsabilidade por perdas e/ou danos decorrentes das infrações cometidas;

12.8 Os custos correspondentes a danos e/ou prejuízos causados por culpa ou dolo da **CONTRATADA** deverão ser ressarcidos ao **CONTRATANTE** no prazo máximo de 05 (cinco) dias úteis, contados da notificação administrativa, sob pena de, sem prejuízo do ressarcimento, serem considerados como hipótese de inadimplemento contratual, sujeita, portanto, à aplicação das sanções administrativas previstas nesta Cláusula.

CLÁUSULA DÉCIMA TERCEIRA – DA RESCISÃO

13.1 A inexecução total ou parcial do Contrato ensejará a sua rescisão, com as consequências contratuais previstas no Capítulo IX, Seção VIII - Da Inexecução e da Rescisão dos Contratos, da Lei Estadual-BA nº 9.433/2005;

13.2 O **CONTRATANTE** poderá rescindir unilateral e administrativamente o presente Contrato, nas hipóteses previstas nos incisos I a XVI, XX e XXI do art. 167 da Lei Estadual-BA nº 9.433/2005;

13.3 Havendo rescisão administrativa do presente contrato, baseada em alguma das hipóteses previstas nos incisos II a XII do art. 167 da Lei Estadual-BA nº 9.433/2005, o **CONTRATANTE** poderá adotar, no que couber, quaisquer das medidas discriminadas no art. 169 do supracitado diploma legal.

CLÁUSULA DÉCIMA QUARTA – DA VINCULAÇÃO AO PROCESSO DE DISPENSA DE LICITAÇÃO

Integram o presente contrato, como se nele estivessem transcritas, as cláusulas e condições estabelecidas no processo de dispensa de Licitação que o originou, referido no preâmbulo deste instrumento, bem como a proposta da **CONTRATADA** apresentada no referido expediente, naquilo que não divirja deste ajuste.

CLÁUSULA DÉCIMA QUINTA – DA PUBLICIDADE

[redacted]

MARIA MAGALI [redacted]

Anexo Contrato assinado SGA (0232606) SEI 19.09.02684.0011790/2021-22 / pg. 805

O **CONTRATANTE** será responsável pela publicação do resumo deste instrumento no Diário da Justiça Eletrônico (DJ-e) do Poder Judiciário do Estado da Bahia, no prazo de 10 (dez) dias corridos, contados a partir da sua assinatura.

CLÁUSULA DÉCIMA SEXTA – DO FORO

Fica eleito o Foro da Cidade do Salvador-Bahia, que prevalecerá sobre qualquer outro, por mais privilegiado que seja, para dirimir quaisquer dúvidas oriundas do presente Contrato.

CLÁUSULA DÉCIMA SÉTIMA – DAS DISPOSIÇÕES GERAIS

17.1 O **CONTRATANTE** não responderá por quaisquer compromissos assumidos perante terceiros pela **CONTRATADA**, ou seus prepostos, ainda que vinculados à execução do presente Contrato;

17.2 A inadimplência da **CONTRATADA**, com relação a quaisquer custos, despesas, tributos, exigências ou encargos previstos neste contrato, não transfere ao **CONTRATANTE** a responsabilidade pelo seu pagamento, nem poderá onerar o objeto do contrato.

17.3 Aplicar-se-á a Lei Estadual-BA nº 9.433/2005 para dirimir toda e qualquer questão legal relativa à execução deste contrato, em especial os casos omissos.

17.4 Fica assegurado ao **CONTRATANTE** o direito de alterar unilateralmente o Contrato, mediante justificação expressa, nas hipóteses previstas no inciso I do art. 143, para melhor adequação às finalidades de interesse público, desde que mantido o equilíbrio econômico-financeiro original do contrato e respeitados os demais direitos da **CONTRATADA**.

17.5 Não caracterizam novação eventuais variações do valor contratual resultantes de revisão de preços, de compensações financeiras decorrentes das condições de pagamento nele previstas ou, ainda, de alterações de valor em razão da aplicação de penalidades.

17.6 Inexistindo disposição específica, as obrigações contratuais devem ser praticadas no prazo de 05 (cinco) dias.

E, por assim estarem justos e acordados, assinam o presente Contrato em 02 (duas) vias, de igual teor e forma, para que produza seus efeitos legais, após a publicação depois de lido e achado conforme.

Salvador, 05 de novembro de 2021.

[redacted] SILVEIRA [redacted]

Ministério Público do Estado da Bahia
Frederico Welington Silveira Soares
Superintendente de Gestão Administrativa

MARIA MAGALI [redacted]

Stefanini Rafael Segurança e Defesa S.A.
Maria Magali Bredariol
Representante Legal

Anexo Contrato assinado SGA (0232606) SEI 19.09.02684.0011790/2021-22 / pg. 806

Anexo Contrato assinado SGA (0232606) SEI 19.09.02684.0011790/2021-22 / pg. 807

MINISTÉRIO PÚBLICO
DO ESTADO DA BAHIA

APENSO I
TERMO DE COMPROMISSO, SIGILO E CONFIDENCIALIDADE

Os abaixo-assinados, de um lado o **MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA**, CNPJ nº 04.142.491/0001-66, situado na cidade de Salvador, a 5ª Avenida, nº 750, Centro Administrativo da Bahia - CAB, doravante denominada **CONTRATANTE**, e de outro lado a **EMPRESA STEFANINI RAFAEL SEGURANÇA E DEFESA S.A.**, CNPJ nº 24.691.488/0001-09, estabelecida à Avenida Eusebio Matoso, nº 1375, Andar 8, Salas 801 e 802, Butantã, CEP 05423-905, São Paulo/SP, doravante denominada **CONTRATADA**, tem entre si justa e acertada, a celebração do presente **TERMO DE COMPROMISSO, SIGILO E CONFIDENCIALIDADE**, através do qual a **CONTRATADA** aceita não divulgar, salvo com autorização prévia e formal, segredos e informações sensíveis de propriedade do **CONTRATANTE,** e se compromete a praticar procedimentos de segurança da informação, em conformidade com as seguintes cláusulas e condições:

1. A **CONTRATADA** compromete-se a manter em caráter confidencial as informações abaixo mencionadas, mesmo após a eventual rescisão do contrato:

1.1 Política de segurança adotada pelo **CONTRATANTE** e configurações de hardware e software decorrentes;

1.2 Processo de instalação, configuração e customizações de produtos, ferramentas e equipamentos e atendimento aos itens de segurança, constantes do Edital de licitação;
1.3 Processo de implantação no ambiente do **CONTRATANTE**, de mecanismos de criptografia e autenticação utilizados;

1.4 Recomendações e implementações decorrentes do processo de consultoria;

1.5 Quaisquer dados que a **CONTRATADA** venha a ter conhecimento em decorrência da presente contratação, pertinentes a hardware, serviços e sistemas aplicativos do **CONTRATANTE**, cujo conhecimento por terceiros exponha o ambiente a riscos de invasão ou resulte na vulnerabilidade do mesmo.

1.6 Não fazer uso das informações prestadas pela **CONTRATANTE** que não seja em absoluto cumprimento ao contrato em questão.

2. A quebra da confidencialidade ou sigilo de informações obtidas na prestação de serviços ensejará multa, responsabilidade criminal na forma da lei, sem prejuízo de outras providências nas demais esferas. A **CONTRATADA** obriga-se a tomar as providências necessárias para assegurar que as informações confidenciais não sejam divulgadas por seus empregados ou agentes.

3. A **CONTRATADA** deve assegurar que todos os seus colaboradores envolvidos diretamente nas atividades objeto da presente contratação guardarão sigilo sobre as informações que porventura tiverem acesso, e que os mesmos se comprometerão a informar, imediatamente, ao seu superior hierárquico, qualquer violação das regras de sigilo, por parte dele ou de qualquer pessoa, inclusive nos casos de violação não intencional.

[redacted]
59
-03'00'

MARIA MAGALI [redacted]

Anexo Contrato assinado SGA (0232606) SEI 19.09.02684.0011790/2021-22 / pg. 808

4. A **CONTRATADA** deverá seguir a Política de Segurança da Informação definida pelo **CONTRATANTE**.

5. O não cumprimento de quaisquer das cláusulas deste Termo implicará em responsabilização administrativa, civil e criminal, de acordo com a legislação vigente.

Em, 05 de novembro de 2021.

FREDERICO WELINGTON SILVEIRA SOARES [redacted] Dados: 2021.11.10 13:04:26 -03'00'

Ministério Público do Estado da Bahia
Frederico Welington Silveira Soares
Superintendente
CONTRATANTE

MARIA MAGALI [redacted]

Stefanini Rafael Segurança e Defesa S.A.
Maria Magali Bredariol
Representante Legal
CONTRATADA

Anexo Contrato assinado SGA (0232606) SEI 19.09.02684.0011790/2021-22 / pg. 809

MINISTÉRIO PÚBLICO
DO ESTADO DA BAHIA

PORTARIA

PORTARIA Nº 339/2021

O **SUPERINTENDENTE DE GESTÃO ADMINISTRATIVA DO MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA**, no uso de suas atribuições, **RESOLVE** designar os servidores Iaçanã Lima de Jesus Carneiro, matrícula nº 351.671, e Plinio Andrade Passos, matrícula nº 354.175, para exercerem as atribuições de fiscal e suplente, respectivamente, do contrato nº 111/2021-SGA, relativo a prestação de serviços técnicos, na área de tecnologia da informação, para a varredura de vulnerabilidades e testes de intrusão PENTEST na aplicação WEB VOTO DIGITAL, no formato Black Box

Superintendência de Gestão Administrativa do Ministério Público do Estado da Bahia.

Frederico Welington Silveira Soares
Superintendente de Gestão Administrativa

Documento assinado eletronicamente por **Frederico Welington Silveira Soares** em 17/11/070192s 1, à 19conforme art. 1º9III9"b"9da Lei 11.: 14/0776.

A autenticidade do documento pode ser conferida no site https‌a‌/sei.sistemas.mpba.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=7 informando o código verificador **0232740** e o código CRC **B98BB17F**.

DIRETORIA DE CONTRATOS, CONVÊNIOS E LICITAÇÕES

AUTORIZAÇÃO PARA INEXIGIBILIDADE DE LICITAÇÃO Nº 017/2021-DADM. Processo SEI: 19.09.02345.0016988/2021-08. Parecer Jurídico: 589/2021. Partes: Ministério Público do Estado da Bahia, e Consultre Consultoria E Treinamento Ltda, CNPJ nº 36.003.671/0001-53. Objeto: Inscrição de servidores no Curso "Gestão, Planejamento e Organização de almoxarifado na Administração Pública", modalidade EAD. Valor: R$ 1.694,00 (mil, seiscentos e noventa e quatro reais). Dotação Orçamentária: Unidade Orçamentária/Gestora: 40.101.0003 - Ação (P/A/OE) 2000 - Região 9900 - Destinação de Recursos 100 - Natureza de Despesa 33.90.39. Fundamento legal: Art. 60, II, § 2º c/c artigo 23, VI, ambos da Lei Estadual nº 9.433/2005.

RESUMO DE CONTRATO DE PRESTAÇÃO DE SERVIÇOS – Nº 111/2021- SGA. Processo SEI: 19.09.02684.0011790/2021-22 - Dispensa nº 004/2021 – DTI. Parecer jurídico: 524/2018. Partes: Ministério Público do Estado da Bahia e empresa Stefanini Rafael Segurança e Defesa S.A., CNPJ nº 24.691.488/0001-09. Objeto: prestação de serviços técnicos, na área de tecnologia da informação, para a varredura de vulnerabilidades e testes de intrusão – PENTEST – na aplicação WEB VOTO DIGITAL, no formato Black Box. Regime de execução: Empreitada por preço global. Valor global: R$ 8.202,67 (oito mil, duzentos e dois reais e sessenta e sete centavos). Dotação orçamentária: Unidade Orçamentária/Gestora 40.601/0003 - Ação (P/A/OE) 2002 - Região 9900 - Destinação de Recursos 100 - Natureza de Despesa 33.90.40. Forma de Pagamento: ordem bancária para crédito em conta corrente do Contratado. Prazo de vigência: 90 (noventa) dias, contados da publicação do resumo no Diário da Justiça Eletrônico.

PORTARIA Nº 339/2021

O SUPERINTENDENTE DE GESTÃO ADMINISTRATIVA DO MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA, no uso de suas atribuições, RESOLVE designar os servidores Iaçanã Lima de Jesus Carneiro, matrícula nº 351.671, e Plinio Andrade Passos, matrícula nº 354.175, para exercerem as atribuições de fiscal e suplente, respectivamente, do contrato nº 111/2021-SGA, relativo a prestação de serviços técnicos, na área de tecnologia da informação, para a varredura de vulnerabilidades e testes de intrusão – PENTEST – na aplicação WEB VOTO DIGITAL, no formato Black Box.

Superintendência de Gestão Administrativa do Ministério Público do Estado da Bahia, 10 de novembro de 2021.

Frederico Welington Silveira Soares
Superintendente de Gestão Administrativa

RESUMO DE CONTRATO DE PRESTAÇÃO DE SERVIÇOS – Nº 117/2021- SGA. Processo SEI: 19.09.00857.0014161/2021-08 - Dispensa nº 071/2021 – DTI. Parecer jurídico: 533/2021. Partes: Ministério Público do Estado da Bahia e empresa Sompo Seguros S/A., CNPJ nº 61.383.493/0001-80. Objeto: prestação de serviços de seguro contra incêndio, queda de raio, explosão de qualquer natureza, danos elétricos e demais coberturas adicionais para imóvel de propriedade do Ministério Público do Estado da Bahia, situado no centro administrativo da Bahia, pelo período de 365 (trezentos e sessenta e cinco) dias. Regime de execução: Empreitada por preço global. Valor global: R$ 10.047,30 (dez mil e quarenta e sete reais e trinta centavos). Dotação orçamentária: Unidade Orçamentária/Gestora 40.101/0003 - Ação (P/A/OE) 2000 - Região 9900 - Destinação de Recursos 100 - Natureza de Despesa 33.90.39. Forma de Pagamento: ordem bancária para crédito em conta corrente do Contratado. Prazo de vigência: 365 (trezentos e sessenta e cinco) dias, a começar às 24 horas do dia 09 de novembro de 2021 e a terminar às 24 horas do dia 09 de novembro de 2022.

PORTARIA Nº 340/2021

O SUPERINTENDENTE DE GESTÃO ADMINISTRATIVA DO MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA, no uso de suas atribuições, RESOLVE designar as servidoras Milena de Carvalho Oliveira Côrtes, matrícula nº 352.739, e Mariana de Araújo Pimentel, matrícula nº 354.027, para exercerem as atribuições de fiscal e suplente, respectivamente, do contrato nº 117/2021-SGA, relativo à prestação de serviços de SEGURO CONTRA INCÊNDIO, QUEDA DE RAIO, EXPLOSÃO DE QUALQUER NATUREZA, DANOS ELÉTRICOS E DEMAIS COBERTURAS ADICIONAIS para imóvel de propriedade do Ministério Público do Estado da Bahia, situado no Centro Administrativo da Bahia, pelo período de 365 (trezentos e sessenta e cinco) dias.

Superintendência de Gestão Administrativa do Ministério Público do Estado da Bahia, 10 de novembro de 2021.

Frederico Welington Silveira Soares
Superintendente de Gestão Administrativa

RESUMO DE CONTRATO DE PRESTAÇÃO DE SERVIÇOS – Nº 115/2021- SGA. Processo SEI: 19.09.00925.0015663/2021-41 - Dispensa nº 006/2021 – DTI. Parecer jurídico: 874/2018. Partes: Ministério Público do Estado da Bahia e empresa Agnaldo Lucas da Silva, CNPJ nº 25.017.607/0001-05. Objeto: prestação de serviços de jardinagem para a Promotoria de Justiça Regional de Barreiras. Regime de execução: Empreitada por preço unitário. Valor global: R$ 6.000,00 (seis mil reais). Dotação orçamentária: Unidade Orçamentária/Gestora 40.101/0022 - Ação (P/A/OE) 4058 - Região 6300 - Destinação de Recursos 100 - Natureza de Despesa 33.90.39. Forma de Pagamento: ordem bancária para crédito em conta corrente do Contratado. Prazo de vigência: 12 (doze) meses, a contar de 16 de novembro de 2021 até 15 de novembro de 2022.

MINISTÉRIO PÚBLICO
DO ESTADO DA BAHIA

DESPACHO

Encaminhamos o expediente à Diretoria de Tecnologia da Informação, acompanhado da publicação do resumo do Contrato nº 111/2021-SGA no Diário da Justiça Eletrônico nº 2.979, do dia 12/11/2021.

Oportunamente, encaminhamos também a publicação da Portaria nº 339/2021, designatória de fiscal e suplente do mencionado ajuste.

Documento assinado eletronicamente por **Paula Souza de Paula** em 29/22/909271s 2, à9: 7con3rme artf 2.7ºº7I" I7da bei 22fL24/9006f

A autenticidade do documento pode ser con3erida no site https:ä/seifsistemasfmp" afmpf" r/sei/controlador_externofphp?acao=documento_con3rir&id_orgao_acesso_externo=0 in3rmando o código veri3cador **0234973** e o código CRC **E10277B7**f

MINISTÉRIO PÚBLICO
DO ESTADO DA BAHIA

MANIFESTAÇÃO

À

DICOFIN

Cumprimentando-os cordialmente, encaminhamos o **PROCESSO DE DISPENSA LICITAÇÃO - SEI Nº 19.09.02684.0011790/2021-22 - STEFANINI,** referente ao mês de **Contrato 111/2021-SGA,** para adoção de providências de pagamento.

Oportunamente, informamos que o referido processo encontra-se relacio ao **PROCESSO DE PAGAMENTO - SEI 20871/2021 - STEFANINI.**

Atenciosamente.

Jorge Alberto dos Santos Conceição

Assistente Técnico Administrativo

Diretoria de Tecnologia da Informação - DTI

Execução Orçamentária

---

sei! assinatura eletrônica

Documento assinado eletronicamente por **Jorge Alberto dos Santos Conceicao** em 03/09/909921s , à:0, 2con4brme artf , .2°°°2I" I2da bei , , fà, L/9006f

---

A autenticidade do documento pode ser con4erida no site https://seifsistemasfmp" afmpf" r/sei/controlador_externofphp?acao=documento_con4erir&id_orgao_acesso_externo=0 in4brmando o código veri4cador **0285278** e o código CRC **A6552EF7**f

---