MINISTÉRIO PÚBLICO
DO ESTADO DA BAHIA

CONTRATO

CONTRATO DE PRESTAÇÃO DE SERVIÇOS – PROCEDIMENTO SEI 19.09.02684.0009580/2025-72.

CONTRATO DE PRESTAÇÃO DE SERVIÇOS QUE ENTRE SI CELEBRAM O MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA E O CENTRO DE PESQUISAS EM INFORMATICA LTDA, NA FORMA ABAIXO:

CONTRATO Nº 095/2025 - 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 **André Luis Sant´Ana Ribeiro**, doravante denominado **CONTRATANTE**, e o **Centro de Pesquisas em Informática Ltda**, CNPJ nº. 40.584.096/0002-88, estabelecida à Av. Santos Dumont, 6216, S331 Quadra única, Loteamento Jardim Santo Antônio, Pitangueiras, Lauro de Freitas/BA, CEP 42.701-260, representada por seu sócio - diretor Sr. **João Gualberto Rizzo Araújo,** inscrito no CPF/MF sob o nº 50*******20, doravante denominada **CONTRATADA**, com supedâneo no quanto disposto na Lei Federal nº 14.133/2021 e na Lei Estadual/Ba nº 14.634/2023, e, ainda, observado o constante no Processo de Licitação, **Pregão Eletrônico nº 90015/2025**, protocolado sob o nº 19.09.02684.0009580/2025-72, o qual integra este instrumento independentemente de transcrição, **CELEBRAM** o presente Contrato, mediante as cláusulas e condições seguintes:

CLÁUSULA PRIMEIRA - DO OBJETO

1.1 O presente instrumento tem por objeto contratação de empresa para prestação de serviços Gerenciados de Soluções de Segurança para proteção dos dispositivos, estações de trabalho e servidores, incluindo capacidade estendida de prevenção, detecção e resposta, acesso remoto seguro, gestão de vulnerabilidades, visibilidade, garantias de conformidade, controle de acesso e automação, não apenas para os dispositivos, mas também para os usuários, bem como serviços de instalação, treinamento, gerenciamento, manutenção e atualização das soluções, garantias de conformidade e resposta a incidentes para a equipe do Ministério Público do Estado da Bahia, em regime 24x7, com atendimento on-site, conforme condições estabelecidas neste instrumento;

1.2 A **CONTRATADA** se declara em condições de prestar o serviço objeto deste instrumento em estrita observância com o disposto neste contrato.

1.3 A assinatura do presente instrumento contratual, pela **CONTRATADA**, importa na presunção de plena ciência e aquiescência com o seu conteúdo, inclusive quanto aos documentos anexos.

CLÁUSULA SEGUNDA – DA VINCULAÇÃO AO EDITAL DO CERTAME LICITATÓRIO

Integram o presente contrato, vinculando esta contratação, independentemente de transcrição: o termo de referência, a proposta da contratada e eventuais anexos dos documentos supracitados, além das condições estabelecidas no edital do certame, que o originou, referido no preâmbulo deste instrumento.

CLÁUSULA TERCEIRA – DA DURAÇÃO DO CONTRATO

3.1 O prazo de vigência do presente Contrato é de 36 (trinta e seis) meses, a contar da data da (última) assinatura pelas partes, admitindo-se a sua prorrogação por sucessivos períodos, limitados a 10 (dez) anos, nos termos dos artigos 106 e 107 c/c artigo 6º, XV da Lei Federal nº 14.133/2021, e será formalizada por termo aditivo;

3.1.1 A prorrogação de que trata este dispositivo é condicionada ao ateste, pela autoridade competente, de que as condições e os preços permanecem vantajosos para a Administração, permitida a negociação com a **CONTRATADA**;

3.1.2 A prorrogação do prazo de vigência contratual fica condicionada, ademais, à disponibilidade orçamentária, devidamente declarada pela Unidade Gestora do recurso nos autos do procedimento administrativo correspondente.

CLÁUSULA QUARTA - DO REGIME, DA FORMA DE EXECUÇÃO E DOS PRAZOS PARA EXECUÇÃO

4.1 O Regime de execução do presente Contrato é de Execução Indireta na modalidade Empreitada por Preço Global;

4.2 O **CONTRATANTE** convocará a **CONTRATADA** para retirar a nota de empenho no prazo de até 05 (cinco) dias corridos contado a partir da notificação pela Administração, que ocorrerá, preferencialmente, através de envio de e-mail para o endereço indicado na proposta de preços;

4.2.1 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).

4.2.2 A Contratada poderá solicitar a prorrogação do prazo para retirada/recebimento da nota de empenho, por motivo justo e aceito pela Administração.

4.3 Os serviços deverão ser executados no seguinte endereço: Sede Administrativa: 5ª Avenida, n° 750, do CAB - Salvador no horário das 8:00h às 12h e das 14h às 18h endereço, em dias expediente administrativo – segunda a sexta;

4.4 Para realização dos serviços é necessário o prévio agendamento juntamente com a Diretoria de Tecnologia da Informação – Coordenação de Assessoramento em

Segurança da Informação, através dos contatos (071 3103-0214 e iassa@mpba.mp.br. A Diretoria de Tecnologia da Informação – Coordenação de Assessoramento em Segurança da Informação é o responsável por acompanhar a execução;

4.5 O prazo de início de execução do objeto é de até 30 (trinta) dias úteis contados do dia útil subsequente ao recebimento da Nota de Empenho, Contrato ou documento equivalente;

4.6 Os serviços serão prestados nas seguintes condições:

Serviços/Etapas	**Condições**	**Cronograma de Execução**
01	Entrega do licenciamento	5 dias
02	Kick off, preparação das máquinas virtuais, planejamento/execução de possíveis implantação das soluções migrações,	20 dias
03	Treinamento	5 dias

4.7 Devidamente justificado e com pelo menos 15 dias corridos de antecedência do prazo final de execução, o prestador de serviço poderá solicitar prorrogação de prazo, ficando a cargo da área demandante acolher a solicitação, desde que não haja prejuízo, ressalvadas situações de caso fortuito e força maior;

4.8 Para a perfeita execução dos serviços, o prestador do serviço deverá disponibilizar os materiais, equipamentos, ferramentas e utensílios necessários, nas quantidades estimadas e qualidades a seguir estabelecidas, promovendo sua substituição quando necessário;

4.9 O prestador de serviço se obriga a executar o objeto em conformidade com as especificações descritas na Proposta de Preços e neste Termo de Referência, sendo de sua inteira responsabilidade a substituição, caso não esteja em conformidade com as referidas especificações;

4.10 Todas as despesas relativas à execução do objeto licitado, bem como todos os impostos, taxas e demais despesas decorrentes do futuro contrato correrão por conta exclusiva do prestador de serviço;

4.11 Demais especificações técnicas relativas à solução encontram-se detalhadas nas especificações técnicas detalhadas.

CLÁUSULA QUINTA – DO RECEBIMENTO DO OBJETO

5.1 O recebimento provisório dos serviços será realizado mediante termo detalhado emitido pelo fiscal técnico, relativamente ao cumprimento dos prazos de execução e demais exigências de caráter técnico, devendo ocorrer em até 05 (cinco) dias corridos;

5.1.1 O prazo de que trata o subitem anterior será contado do recebimento de comunicação escrita do fornecedor com a comprovação da prestação dos serviços a que se refere a parcela a ser paga;

5.2 Os serviços poderão ser rejeitados, no todo ou em parte, inclusive antes do recebimento provisório, quando em desacordo com as especificações constantes neste Termo de Referência e na Proposta de preços, devendo ser refeitos no prazo de 05 (cinco) dias corridos, a contar da intimação do fornecedor, às suas custas, sem prejuízo da aplicação das penalidades, cabendo à fiscalização não atestar o recebimento até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório;

5.3 Quando a fiscalização for exercida por um único servidor, o termo detalhado de recebimento provisório deverá conter o registro, a análise e a conclusão sobre todas as ocorrências na execução do Contrato, acompanhado dos demais documentos que julgar necessários, encaminhando-o ao servidor ou comissão designada pela autoridade competente para recebimento definitivo.

5.4 Os serviços serão recebidos definitivamente, em até 20 (vinte dias) dias corridos], contados do recebimento provisório, pelo gestor do contrato ou comissão designada pelo Superintendente de Gestão Administrativa, mediante termo detalhado que comprove o atendimento de todas as exigências contratuais.

5.5 O prazo para recebimento definitivo poderá ser excepcionalmente prorrogado, de forma justificada, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais.

5.6 Caso necessário, o gestor do contrato notificará o fornecedor, para realização das substituições e/ou adequações cabíveis, conforme prazo indicado no **item 5.2**;

5.7 Para efeito de recebimento provisório, ao final de cada período de faturamento, o(s) fiscal(is) do contrato deverá(ão) apurar o resultado das avaliações da execução do objeto e, se for o caso, a análise do desempenho e qualidade da prestação dos serviços realizados em consonância com os indicadores previstos;

5.7.1 A análise do desempenho e qualidade da prestação dos serviços referida no subitem anterior poderá resultar no redimensionamento de valores a serem pagos ao fornecedor, circunstância que deverá ser registrada pelo(s) fiscal(is) em relatório(s) a ser encaminhado ao gestor do Contrato;

5.8 A fiscalização não efetuará o ateste da última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas durante o recebimento provisório;

5.9 O MPBA rejeitará, no todo ou em parte, inclusive antes do recebimento provisório, o objeto contratual em desacordo com as condições pactuadas, podendo, entretanto, se lhe convier, decidir pelo recebimento, neste caso com as deduções cabíveis;

5.10 Em caso de recusa, no todo ou em parte, do objeto contratado, fica o fornecedor obrigado a substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, conforme prazo indicado no **item 5.2**, cabendo ao Gestor do Contrato somente habilitar para pagamento a(s) parcela(s) recebida(s) em conformidade;

5.11 O recebimento definitivo do objeto deste instrumento será concretizado depois de adotados, pelo MPBA, todos os procedimentos cabíveis em Ato Normativo próprio, no art. 140 da Lei Federal nº 14.133/2021 e, no que couber, da Lei Estadual de nº 14.634/2023, devendo ocorrer no prazo indicado no **item 5.4;**

5.12 Nenhum prazo de recebimento ocorrerá enquanto pendente a solução, pela contratada, de inconsistências verificadas na execução do objeto ou nota(s) fiscal(is) ou instrumento(s) de cobrança equivalente(s);

5.13 O aceite ou aprovação do objeto pelo MPBA não exclui a responsabilidade do fornecedor pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do Contrato; **CLÁUSULA SEXTA – DO PREÇO**

6.1 O preço unitário estabelecido para a plena execução do objeto contratual se encontra descrito na tabela abaixo:

ITEM	DESCRIÇÃO DO SERVIÇO	UNIDADE DE MEDIDA	QUANTIDADE	PREÇO UNITÁRIO	PREÇO TOTAL
1	Serviços gerenciados de soluções de segurança para plataforma SSE com controle de acesso remoto, pelo período de 36 meses	Unidade	500	R$ 1.535,46	R$ 767.730,00
2	Serviços gerenciados de Gestão de exposição cibernética por 36 meses	Unidade	4500	R$ 1.017,26	R$ 4.577.670,00
3	Serviços gerenciados de visibilidade, conformidade, segurança e orquestração dos dispositivos conectados à rede corporativa por 36 meses	Unidade	4000	R$ 409,00	R$ 1.636.000,00
VALOR GLOBAL					R$ 6.981.400,00

6.2 Dá-se ao presente Contrato o valor global de **R$ 6.981.400,00 (seis milhões novecentos e oitenta e um mil e quatrocentos reais)**, equivalente ao período total de vigência da contratação;

6.3 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 da **CONTRATADA** envolvido na execução do objeto, materiais empregados, inclusive ferramentas e fardamentos, combustíveis, lubrificantes, manutenção, lavagens, estacionamento, depreciação, aluguéis, seguros, franquias, administração, tributos e emolumentos.

CLÁUSULA SÉTIMA - DO PAGAMENTO E DA ATUALIZAÇÃO MONETÁRIA

7.1 Os pagamentos serão processados conforme ordem cronológica de pagamento, nos termos disciplinados no art.141 da Lei Federal de nº14.133/21;

7.2 O faturamento referente ao objeto deste contrato será efetuado em 03 (três) parcelas anuais de igual valor, correspondentes ao percentual de 33,33% do serviço total;

7.3 O pagamento será processado mediante apresentação, pela **CONTRATADA**, de fatura, Nota Fiscal relativa à prestação dos serviços e certidões de regularidade cabíveis, bem como consulta à situação de idoneidade da
CONTRATADA, documentação que deverá estar devidamente acompanhada do **TERMO DE RECEBIMENTO** pelo **CONTRATANTE**;

7.4 Os pagamentos serão processados no prazo de 20 (vinte) dias úteis, a contar da data de apresentação da documentação indicada no **item 7.3**, desde que não haja pendência a ser regularizada;

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

7.4.2 No caso de controvérsia sobre a execução do objeto, quanto a dimensão, qualidade e quantidade, a parcela incontroversa deverá ser liberada no prazo previsto para pagamento;

7.5 As faturas far-se-ão acompanhar da documentação probatória relativa ao recolhimento dos tributos que tenham como fato gerador o objeto consignado na **Cláusula Primeira**;

7.6 O **CONTRATANTE** realizará a retenção de impostos ou outras obrigações de natureza tributária, de acordo com a legislação vigente;

7.7 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;

7.8 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 nos **itens 7.4 e 7.4.1.**

7.8.1 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**.

7.9 No ato de liquidação da despesa, os serviços de contabilidade comunicarão aos órgãos da administração tributária as características da despesa e os valores pagos, conforme o disposto no art. 63 da Lei nº 4.320, de 17 de março de 1964.

CLÁUSULA OITAVA – DA MANUTENÇÃO DO EQUILÍBRIO ECONÔMICO-FINANCEIRO DO CONTRATO

8.1 A concessão de reajustamento ocorrerá após o transcurso do prazo de 01 (um) ano da data do orçamento estimado pela Administração, qual seja, 09 de abril de 2025, mediante aplicação do IPCA relativo ao período decorrido entre a referida data e a data da efetiva concessão do reajuste;

8.1.1 Nos reajustes subsequentes ao primeiro, o interregno mínimo de 01 (um) ano será contado a partir dos efeitos financeiros do último reajuste;

8.1.2 Os valores reajustados incidirão sobre as parcelas de serviços a serem executadas após o prazo de que cuida o item 8.1;

8.1.3 A variação do valor contratual para fazer face ao reajuste de preços será realizada por simples apostila, dispensando a celebração de aditamento;

8.2 O reestabelecimento do equilíbrio econômico-financeiro dependerá de requerimento da Contratada quando visar recompor o preço que se tornou insuficiente, devendo ser instruído com a documentação que comprove o desequilíbrio econômico-financeiro do contrato;

8.2.1. O requerimento de restabelecimento do equilíbrio econômico-financeiro inicial do contrato, nas hipóteses do art. 124, II, “d”, ou do art. 135 da Lei Federal nº

14.133, de 2021, deverá ser formulado pelo interessado no prazo máximo de um ano do fato que o ensejou, sob pena de decadência, em consonância com o art. 211 da Lei Federal nº 10.406, de 10 de janeiro de 2002;

8.2.2. Na hipótese de contratos de fornecimento contínuos, o requerimento de restabelecimento do equilíbrio econômico-financeiro deverá ser formulado durante a vigência do contrato e antes de eventual prorrogação nos termos do art. 131, parágrafo único, da Lei n° 14.133, de 2021, sob pena de preclusão;

8.2.2.1. Fica convencionado que, nos casos de contrato de fornecimento contínuos com prazo de vigência superior a 1 (um) ano, o requerimento de restabelecimento do equilíbrio econômico-financeiro do contrato deverá observar a disposição do **subitem 8.2.1**;

8.3 O **CONTRATANTE**, no prazo máximo de 60 (sessenta) dias, prorrogável por igual período mediante justificativa, responderá a eventuais pedidos de manutenção do equilíbrio econômico-financeiro do Contrato apresentado pela Contratada (art. 92, inciso XI, c/c 123, parágrafo único da Lei n° 14.133, de 2021);

8.4 O processo de reestabelecimento do equilíbrio econômico-financeiro em favor do Contratante deverá ser instaurado quando possível a redução do preço ajustado para compatibilizá-lo ao valor de mercado ou quando houver diminuição, devidamente comprovada, dos preços dos insumos básicos utilizados no Contrato.

CLÁUSULA NONA - 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
40.101/0021	2002	9900	1.500.0.100.000000.00.00.00	33.90.40

CLÁUSULA DÉCIMA - DO MODELO DE GESTÃO E FISCALIZAÇÃO CONTRATUAL

10.1 Na forma das disposições estabelecidas na Lei Federal nº 14.133/2021 e na Lei Estadual/BA nº 14.634/2023, o **CONTRATANTE** designará servidor(es), por meio de Portaria específica para tal fim, para a gestão e 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.

10.2 Incumbe à fiscalização acompanhar e verificar a perfeita execução do contrato, em todas as suas fases, competindo-lhe, primordialmente:

10.2.1 Acompanhar o cumprimento dos prazos de execução descritos neste instrumento, e determinar as providências necessárias à correção de falhas, irregularidades e/ou defeitos, sem prejuízos das sanções contratuais legais;

10.2.2 Transmitir à **CONTRATADA** as instruções, e comunicar alterações de prazos ou roteiros, quando for o caso;

10.2.3 Promover, com a presença da **CONTRATADA**, a verificação dos serviços já efetuados;

10.2.4 Esclarecer as dúvidas da **CONTRATADA**, solicitando ao setor competente do **CONTRATANTE**, se necessário, parecer de especialistas;

10.2.5 Manter anotação em registro próprio todas as ocorrências relacionadas à execução do contrato, determinando o que for necessário para a regularização das faltas ou dos defeitos observados;

10.2.6 Informar aos seus superiores, em tempo hábil para a adoção das medidas convenientes, a situação que demandar decisão ou providência que ultrapasse sua competência (Lei Estadual de nº14.634/23; art.12, §2º e Lei nº 14.133/2021, art. 117, §2º);

10.3 A fiscalização, pelo **CONTRATANTE**, não desobriga a **CONTRATADA** de sua responsabilidade quanto à perfeita execução do objeto contratual;

10.3.1 A ausência de comunicação, por parte do **CONTRATANTE**, sobre irregularidades ou falhas, não exime a **CONTRATADA** das responsabilidades determinadas neste contrato;

10.4 O **CONTRATANTE** poderá recusar, sustar e/ou determinar o desfazimento/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 ainda que atentem contra a segurança de terceiros ou de bens;

10.4.1 Qualquer serviço considerado não aceitável, no todo ou em parte, deverá ser refeito pela **CONTRATADA**, às suas expensas;

10.4.2 A não aceitação de algum serviço, no todo ou em parte, não implicará na dilação do prazo de execução, salvo expressa concordância do **CONTRATANTE**;

10.5 Caberá ao gestor do contrato deliberar sobre a execução contratual, em especial:

10.5.1 Autorizar o início da execução do objeto contratual, deliberando sobre o momento do envio de documentos de formalização tais como documentos ou nota de empenho ordinária à contratada;

10.5.2 Coordenar as atividades realizadas pelos fiscais técnico, administrativo e setorial quanto ao cumprimento de obrigações assumidas pela contratada, elaborando, sempre que necessário, relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento à finalidade da Administrativa;

10.5.3 Receber dúvidas ou questionamentos de matérias sob sua competência, feitos pelo fornecedor e/ou pela fiscalização, manifestando-se e dando o devido encaminhamento;

10.5.4 Deliberar sobre prorrogações de prazos de entre ou execução;

10.5.5 Deliberar sobre o recebimento definitivo do objeto contratado, mediante emissão de termo detalhado, quando não for designada comissão específica para tal fim;

10.5.6 Adotar as providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso;

10.6 Para fins de fiscalização e gestão o MPBA poderá solicitar ao fornecedor, a qualquer tempo, os documentos relacionados com a execução do futuro contrato;

10.7 A gestão e a fiscalização contratual observarão, ainda, as normas e regulamentos internos do Ministério Público do Estado da Bahia que venham a ser publicados para disciplina da matéria.

CLÁUSULA DÉCIMA PRIMEIRA – DAS OBRIGAÇÕES DA CONTRATADA

11.0 Além das determinações contidas na Cláusula **QUARTA** - **do Regime e da forma de execução** deste contrato e no processo de Licitação que o originou – que aqui se consideram literalmente transcritas, bem como daquelas decorrentes de lei, a **CONTRATADA**, obriga-se a:

11.1 Cumprir todas as obrigações constantes no Edital, seus anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto;

11.2 Efetuar a execução do objeto em perfeitas condições, conforme especificações, prazo e local constantes neste Termo de Referência e seus apensos, acompanhado da respectiva nota fiscal com todas as discriminações inerentes ao objeto, bem como as certidões de regularidade cabíveis;

11.3 Responder por quaisquer danos e prejuízos causados em função do objeto do contrato a ser firmado, bem como por todos os danos e prejuízos decorrentes de paralizações na execução dos serviços, salvo na ocorrência de motivo de força maior, apurados na forma da legislação vigente, e desde que comunicados ao MPBA no prazo de 48 horas do fato, ou da ordem expressa escrita do MPBA;

11.4 Reparar, corrigir, remover, reconstruir ou substituir, total ou parcialmente, às suas expensas, no prazo fixado neste Termo de Referência, o objeto do futuro contrato em que se verifiquem má qualidade, vícios, defeitos ou incorreções, resultantes de execução irregular, do emprego de materiais ou equipamentos inadequados, se for o caso, ou não correspondente(s) ao(s) material(is);

11.5 Comunicar ao MPBA, no prazo de 48 horas que antecede a data da execução, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação;

11.6 Manter, durante toda a execução do futuro contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

11.7 Promover a destinação final ambientalmente adequada do dos materiais eventualmente empregados na prestação dos serviços, sempre que a legislação assim o exigir;
11.8 Prestar ao MPBA, sempre que necessário, esclarecimentos, fornecendo toda e qualquer orientação necessária.

11.9 Dispor de toda mão de obra, veículos, transportes, insumos, Alvarás, licenciamentos, autorizações e materiais necessários à execução do objeto deste Termo de Referência;

11.10 Assegurar que o objeto deste Termo de Referência não sofra solução de continuidade durante todo o prazo da sua vigência;

11.11 Responsabilizar-se pelo cumprimento das obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas em legislação específica na execução do objeto, cuja inadimplência não transfere a responsabilidade ao MPBA;

11.12 A eventual retenção de tributos pelo MPBA não implicará a responsabilização deste, em hipótese alguma, por quaisquer penalidades ou gravames futuros, decorrentes de inadimplemento(s) de tributos pelo fornecedor.

11.13 Emitir notas fiscais/faturas de acordo com a legislação, contendo descrição do objeto, indicação de quantidades, preços unitários e valor total, competindo ao fornecedor, ainda, observar, de acordo com a previsão da legislação tributária aplicável, nas hipóteses de retenção de tributos pelo MPBA, a necessidade de seu destaque, se cabível, bem como a discriminação das informações requeridas nas Notas Fiscais, conforme os comandos legais específicos;

11.14 Responsabilizar-se pelos vícios, ainda que ocultos, e danos decorrentes da execução do objeto, bem como por todo e qualquer dano causado à Administração ou terceiros, não reduzindo essa responsabilidade a fiscalização ou o acompanhamento da execução contratual pelo MPBA, que ficará autorizado a descontar dos pagamentos devidos ou da garantia, caso exigida, o valor correspondente aos danos sofridos;

11.15 Atender, nos prazos consignados neste instrumento, às recusas ou determinações, pelo MPBA, de refazimento dos serviços que não estejam sendo ou não tenham sido executados de acordo com o estipulado neste instrumento, providenciando sua imediata correção, sem ônus para o MPBA;

11.15.1 Comunicar ao MPBA, no prazo de 24 (vinte e quatro) horas, qualquer ocorrência anormal relativa à execução;

11.16 Prestar todo esclarecimento ou informação solicitada pelo MPBA ou por seus prepostos, garantindo-lhes o acesso, a qualquer tempo, aos documentos relativos à execução do objeto;

11.17 Não contratar, durante a vigência do futuro contrato, cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, de dirigente do MPBA, ou do fiscal ou do gestor, nos termos do artigo 48, parágrafo único, da Lei 14.133/2021;

11.18 Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do futuro contrato;

11.19 Cumprir, durante todo o período de execução do futuro contrato, a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, bem como as reservas de cargos previstas na legislação (art. 116, da Lei nº 14.133/2021);

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

11.21 Prestar diretamente os serviços ora contratados, não os transferindo a outrem, no todo ou em parte, sendo vedada a subcontratação, ainda que parcial, do objeto contratado.

CLÁUSULA DÉCIMA SEGUNDA – DAS OBRIGAÇÕES DO CONTRATANTE

12.1 **O CONTRATANTE**, além das obrigações contidas neste contrato por determinação legal, obriga-se a:

12.2 Receber os serviços no prazo e condições estabelecidas no Edital e seus anexos;

12.3 Verificar minuciosamente, no prazo fixado, a conformidade dos serviços recebidos provisoriamente com as especificações constantes do Edital e da proposta, para fins de aceitação e recebimento definitivo;

12.4 Comunicar ao fornecedor, por escrito, sobre imperfeições, falhas ou irregularidades verificadas no objeto fornecido, para que seja refeito, reparado ou corrigido;

12.5 Acompanhar e fiscalizar o cumprimento das obrigações do fornecedor, através de comissão/servidor especialmente designado;

12.6 Efetuar o pagamento ao fornecedor no valor correspondente a execução do objeto, no prazo e forma estabelecidos neste instrumento;

12.7 Rejeitar os serviços executados fora das especificações exigidas ou quando não estejam de conformidade com os padrões de qualidade, dando ciência dos motivos da recusa ao fornecedor, que assumirá todas as despesas daí decorrentes.

12.8 Notificar previamente ao fornecedor, quando da aplicação de penalidades;

12.9 Atestar as notas fiscais/faturas emitidas pelo fornecedor, recusando-as quando inexatas ou incorretas, efetuando todos os pagamentos nas condições pactuadas;

12.10 Emitir Ordem de Serviço para instruir a execução dos serviços;

12.11 Rejeitar, no todo ou em parte, os serviços executados em desacordo com as exigências do Termo de Referência e seus anexos.

12.12 Explicitamente emitir decisão sobre todas as solicitações e reclamações relacionadas à execução do presente Contrato, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do ajuste, observando os seguintes prazos:

12.12.1 A administração responderá à contratada dentro dos prazos legalmente estabelecidos, contados da data da conclusão da instrução do requerimento.

CLÁUSULA DÉCIMA TERCEIRA - DO CUMPRIMENTO DA LEI GERAL DE PROTEÇÃO DE DADOS - LEI N. 13.709/2018

13.1 É vedado às partes a utilização de todo e qualquer dado pessoal repassado em decorrência da execução contratual para finalidade distinta daquela do objeto da contratação, mantendo-se sigilo e confidencialidade, sob pena de responsabilização administrativa, civil e criminal;

13.2 A **CONTRATADA** declara que tem ciência da existência da Lei Geral de Proteção de Dados e se compromete a adequar todos os procedimentos internos ao disposto na legislação com o intuito de proteger os dados pessoais repassados pelo **CONTRATANTE**;

13.3 A **CONTRATADA** fica obrigada a comunicar ao **Ministério Público do Estado da Bahia**, em até 24 (vinte e quatro) horas do conhecimento, qualquer incidente de acessos não autorizados aos dados pessoais, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, bem como adotar as providências dispostas no art. 48 da LGPD;

13.4 A **CONTRATADA** cooperará com o **CONTRATANTE** no cumprimento das obrigações referentes ao exercício dos direitos dos titulares previstos na LGPD e nas Leis e Regulamentos de Proteção de Dados em vigor e também no atendimento de requisições e determinações do Poder Judiciário, Ministério Público, ANPD e Órgãos de controle administrativo em geral;

13.5 Eventuais responsabilidades das partes serão apuradas conforme estabelecido neste contrato e também de acordo com o que dispõe a Seção III, Capítulo VI da LGPD.

CLÁUSULA DÉCIMA QUARTA - DA GARANTIA DA EXECUÇÃO

Não será exigida garantia da execução contratual.

CLÁUSULA DÉCIMA QUINTA – DAS INFRAÇÕES E DAS SANÇÕES ADMINISTRATIVAS

15.1 A **CONTRATADA** sujeitar-se-á às sanções administrativas previstas nas Leis Federal nº. 14.133/2021 e Estadual nº 14.634/23, as quais poderão vir a ser aplicadas após o prévio e devido processo administrativo, assegurando-lhe, sempre, o contraditório e a ampla defesa;

15.2 Comete infração administrativa, nos termos da Lei nº 14.133, de 2021, a **CONTRATADA** que:

15.2.1 Der causa à inexecução parcial do contrato;

15.2.2 Der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;

15.2.3 Der causa à inexecução total do contrato;

15.2.4 Não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;

15.2.5 Ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;

15.2.6 Apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;

15.2.7 Não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

15.2.8 Praticar ato fraudulento na execução do contrato;

15.2.9 Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

15.2.10 Praticar ato lesivo previsto no art.5º da Lei nº 12.846, de 1º de agosto de 2013;

15.3 Serão aplicadas ao responsável pelas infrações administrativas acima descritas as seguintes sanções:

15.3.1 **Advertência**, quando a **CONTRATADA** der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, §2º, da Lei Federal nº 14.133/2021);

15.3.2 **Impedimento de licitar e contratar**, quando praticadas as condutas descritas nos itens 15.2.2, a 15.2.4 acima, sempre que não se justificar a imposição de penalidade mais grave (art. 156, §4º, da Lei Federal 14.133/2021);

15.3.3 **Declaração de inidoneidade para licitar e contratar**, quando praticadas as condutas descritas nos itens 15.2.5 a 15.2.10, acima, bem como nas alíneas 15.2.2 a

15.2.4, que justifiquem a imposição de penalidade mais grave (art. 156, §5º, da Lei Federal nº 14.133/21);

15.3.4 Multa:

15.3.4.1 Moratória de 0,5% (meio por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 30 (trinta) dias;

15.3.4.2 Compensatória de 20% (vinte por cento) sobre o valor total do contrato, para as infrações descritas nas alíneas 15.2.6 a 15.2.10;

15.3.4.3 Compensatória de 20% (vinte por cento) sobre o valor total do contrato, para as infrações descritas na alínea 15.2.3 e 15.2.4;

15.3.4.4 Para as infrações constantes das alíneas 15.2.1, 15.2.2 e 15.2.5, a multa será de 20% (vinte por cento) sobre o valor total do contrato;

15.3.4.5 Será admitida medida cautelar destinada a garantir o resultado útil do processo administrativo sancionatório, de forma antecedente ou incidental à sua instauração, inclusive a retenção provisória do valor correspondente à estimativa da sanção de multa;

15.3.4.5.1 O valor da retenção provisória a que se refere o subitem anterior deste artigo não poderá exceder ao limite máximo estabelecido no §3º do art. 156 da Lei Federal nº 14.133, de 2021;

15.4 A aplicação das sanções previstas neste Contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao **CONTRATANTE**;

15.5 Todas as sanções previstas neste Contrato poderão ser aplicadas cumulativamente com a multa;

15.5.1. Antes da aplicação da multa será facultada a defesa do interessado no prazo de **15 (quinze) dias úteis**, contado da data de sua intimação;

15.5.2. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo **CONTRATANTE** à **CONTRATADA**, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente, conforme o caso;

15.5.3. Previamente ao encaminhamento à cobrança judicial, a multa poderá ser recolhida administrativamente no prazo máximo de 30 (trinta) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente;

15.6. A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa aa contratada, observando-se o procedimento previsto no caput e parágrafos do art. 158 da Lei nº 14.133, de 2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar;

15.7. Na aplicação das sanções serão considerados:

15.7.1 A natureza e a gravidade da infração cometida;

15.7.2 As peculiaridades do caso concreto;

15.7.3 As circunstâncias agravantes ou atenuantes;

15.7.4 Os danos que dela provierem para o **CONTRATANTE**;

15.7.5 A implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle;

15.8 Os atos previstos como infrações administrativas na Lei nº 14.133, de 2021, e na Lei Estadual nº 14.634/23, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846, de 2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei;

15.9 A personalidade jurídica da contratada poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Contrato ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com a contratada, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia;

15.10 O **CONTRATANTE** deverá, no prazo máximo 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ela aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no Cadastro Nacional de Empresas Punidas (Cnep), instituídos no âmbito do Poder Executivo Federal;

15.11 As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133/21 e da Lei Estadual de nº 14.634/23;

15.12 Os débitos da contratada para com a Administração contratante, resultantes de multa administrativa e/ou indenizações, não inscritos em dívida ativa, poderão ser compensados, total ou parcialmente, com os créditos devidos pelo referido órgão decorrentes deste mesmo contrato ou de outros contratos administrativos que a contratada possua com o mesmo órgão ora contratante.

CLÁUSULA DÉCIMA SEXTA – DAS ALTERAÇÕES CONTRATUAIS

16.1 Eventuais alterações contratuais reger-se-ão pela disciplina dos arts. 124 e seguintes da Lei nº 14.133, de 2021 e da Lei Estadual de n º 14.634/23;

16.2 A **CONTRATADA** é obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato;

16.3 As alterações contratuais deverão ser promovidas mediante celebração de termo aditivo, submetido à prévia análise da Assessoria Jurídica do **CONTRATANTE**, salvo nos casos de justificada necessidade de antecipação de seus efeitos, hipótese em que a formalização do aditivo deverá ocorrer no prazo máximo de 1 (um) mês;

16.4 Registros que não caracterizem alteração do contrato podem ser realizados por simples apostila, dispensada a celebração do termo aditivo, na forma do artigo 136, da Lei 14.133, de 2021.

CLÁUSULA DÉCIMA SÉTIMA – DA EXTINÇÃO DO CONTRATO

17.1 O contrato se extingue quando vencido o prazo nele estipulado, independentemente de terem sido cumpridas ou não as obrigações de ambas as partes contraentes;

17.1.1. O contrato pode ser extinto antes do prazo nele fixado, sem ônus para o **CONTRATANTE**, quando este não dispuser de créditos orçamentários para sua

continuidade ou quando entender que o contrato não mais lhe oferece vantagem;

17.1.1.2. A extinção nesta hipótese ocorrerá na próxima data de aniversário do contrato, desde que haja a notificação da contratada pelo **CONTRATANTE** nesse sentido com pelo menos 2 (dois) meses de antecedência desse dia;

17.1.1.3. Caso a notificação da não-continuidade do contrato de que trata este subitem ocorra com menos de 2 (dois) meses da data de aniversário, a extinção contratual ocorrerá após 2 (dois) meses da data da comunicação;

17.2 O contrato pode ser extinto antes de cumpridas as obrigações nele estipuladas, ou antes do prazo nele fixado, por algum dos motivos previstos no artigo 137 da Lei Federal nº 14.133/2021, bem como de forma consensual, assegurados o contraditório e a ampla defesa;

17.2.1 A extinção do contrato poderá ser:

a) determinada por ato unilateral e escrito da Administração, exceto no caso de descumprimento decorrente de sua própria conduta (arts. 138, inciso I, da Lei nº 14.133, de 2021);
b) consensual, por acordo entre as partes, por conciliação, por mediação ou por comitê de resolução de disputas, desde que haja interesse da Administração (art. 138, inciso II, da Lei nº 14.133, de 2021);
c) determinada por decisão arbitral, em decorrência de cláusula compromissória ou compromisso arbitral, ou por decisão judicial (art. 138, inciso III, da Lei nº 14.133, de 2021);

17.2.2 A alteração social ou modificação da finalidade ou da estrutura da empresa não ensejará rescisão se não restringir sua capacidade de concluir o contrato;

17.2.2.1 Se a operação implicar mudança da pessoa jurídica **CONTRATADA**, deverá ser formalizado termo aditivo para alteração subjetiva;

17.3 O termo de rescisão, sempre que possível, será precedido:

17.3.1 Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

17.3.2 Relação dos pagamentos já efetuados e ainda devidos;

17.3.3 Indenizações e multas.

17.4 O contrato poderá ser extinto, ainda:

17.4.1 Caso se constate que a contratada mantém vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade **CONTRATANTE** ou com agente público que tenha desempenhado função na licitação no processo de contratação direta ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau;

17.4.2 Caso se constate que a pessoa jurídica **CONTRATADA** possui administrador ou sócio com poder de direção, familiar de detentor de cargo em comissão ou função de confiança que atue na área responsável pela demanda ou contratação ou de autoridade a ele hierarquicamente superior no âmbito do órgão **CONTRATANTE**.

CLÁUSULA DÉCIMA OITAVA – DA PUBLICIDADE

O CONTRATANTE será responsável pela publicação deste instrumento nos termos e condições previstas na Lei nº 14.133/2021.

CLÁUSULA DÉCIMA NONA – 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 VIGÉSIMA – DAS DISPOSIÇÕES GERAIS

20.1 **O CONTRATANTE** não responderá por quaisquer compromissos assumidos perante terceiros pela **CONTRATADA**, ou seus prepostos, ainda que vinculados à execução do presente Contrato;

20.2 A inadimplência da **CONTRATADA**, com relação a quaisquer custos, despesas, tributos, exigências ou encargos, não transfere ao **CONTRATANTE** a responsabilidade pelo seu pagamento, nem poderá onerar o objeto do contrato;

20.3 Os casos omissos serão decididos pelo **CONTRATANTE**, segundo as disposições contidas na Lei Federal nº 14.133, de 2021 e estadual nº 14.634 de 2023 e demais normas federais e estaduais aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei nº 12.078, de 1990 – Código de Defesa do Consumidor – e normas e princípios gerais dos contratos;

20.4 Fica assegurado ao **CONTRATANTE** o direito de alterar unilateralmente o Contrato, mediante justificativa expressa, nas hipóteses previstas na Lei Federal 14.133/21 e na forma de Lei Estadual de nº 14.634/23 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**;

20.5 Não caracterizam novação eventuais variações do valor contratual resultantes de reajustamento/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;

20.6 A Administração não responderá por quaisquer compromissos assumidos pela **CONTRATADA** com terceiros, ainda que vinculados à execução do contrato, bem como por qualquer dano causado a terceiros em decorrência de ato da **CONTRATADA**, de seus empregados, prepostos ou subordinados;

20.7 O presente contrato regula-se pelas suas cláusulas e pelos preceitos de direito público, aplicando-se, supletivamente, os princípios da teoria geral dos contratos e as disposições de direito privado;

E, por assim estarem justos e acordados, assinam o presente Contrato para que produza seus efeitos legais.

Salvador, 2025.

Centro de Pesquisas em Informática Ltda
João Gualberto Rizzo Araújo
sócio - diretor

MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA
André Luis Sant´Ana Ribeiro
Superintendente de Gestão Administrativa

(Assinado e datado eletronicamente/digitalmente)

Documento assinado eletronicamente por **João Gualberto Rizzo Araujo** - Usuário Externo, em 23/07/2025, às 15:45, conforme Ato Normativo n° 047, de 15 de Dezembro de 2020 - Ministério Público do Estado da Bahia.

Documento assinado eletronicamente por **André Luis Sant Ana Ribeiro** - Superintendente, em 24/07/2025, às 10:56, conforme Ato Normativo n° 047, de 15 de Dezembro de 2020 - Ministério Público do Estado da Bahia.

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 **1618715** e o código CRC **0D47859E**.

MINISTÉRIO PÚBLICO
DO ESTADO DA BAHIA

CONTRATO

CONTRATO Nº 095/2025 - SGA

APENSO I
ESPECIFICAÇÕES TÉCNICAS DETALHADAS

OBJETO: Contratação de Serviço Gerenciado de Soluções de Segurança para proteção dos dispositivos, estações de trabalho e servidores, incluindo capacidade estendida de prevenção, detecção e resposta, acesso remoto seguro, gestão de vulnerabilidades, visibilidade, garantias de conformidade, controle de acesso e automação, não apenas para os dispositivos, mas também para os usuários, bem como serviços de instalação, treinamento, gerenciamento, manutenção e atualização das soluções, garantias de conformidade e resposta a incidentes para a equipe do Ministério Público da Bahia em regime 24x7 com atendimento on-site, conforme detalhamento descrito neste documento de especificações técnicas detalhadas, pelo período de 36 meses.

ESPECIFICAÇÕES TÉCNICAS:

1. Item 1 – Serviços Gerenciados de Soluções de Segurança para plataforma SSE com controle de acesso remoto, pelo período de 36 meses

1.1. A plataforma de segurança a ser fornecida na modalidade Software como Serviço (SaaS), deve possuir alinhamento direto com o conceito Security Service Edge do Gartner, mais especificamente para funcionalidade de Acesso remoto seguro: Redirecionamento seguro baseado no conceito Zero Trust Network Access para as aplicações internas posicionadas no ambiente on-premise ou em nuvens públicas.

1.2. CARACTERÍSTICAS GERAIS

1.3. A solução de segurança proposta deverá ser fornecida em uma arquitetura 100% baseada em nuvem.

1.4. O fabricante deverá prover, no mínimo, 3 (três) estruturas de processamento de dados no Brasil para melhor experiência do usuário, garantindo:

1.4.1 Uso global, com mais de 50 pontos no mundo, da infraestrutura do fabricante;

1.4.2 Uso irrestrito de banda por parte dos usuários;

1.4.3 Disponibilidade de 99.999% dos datacenters no Brasil e no mundo;

1.4.4 30 ms para tráfego não criptografado e 70 ms para tráfego criptografado;

1.4.5 Armazenamento de eventos no período mínimo de 90 dias;

1.4.6 Deverá prover 90 dias de retenção de logs na console administrativa;

1.5. O fabricante deverá prover suporte nativo ao Microsoft Active Directory (ADFS) e Microsoft Azure AD (SCIM e SAML v2), para:

1.5.1 Autenticação dos usuários para o Acesso Remoto;

1.5.2 Sincronização de usuários, grupos e OU's;

1.5.3 Single Sign-on para usuários administrativos.

1.6. Os dados dos usuários do MPBA deverão ser logicamente apartados através de arquitetura multi-tenant ofertada pela plataforma;

1.7. Toda inspeção do tráfego deverá ser feita em nuvem, com exceção das exceções de tráfego local e conformidade do dispositivo;

1.8. A solução deverá prover painel único de gestão, contemplando os módulos propostos neste referencial técnico.

1.9. O agente do próprio fabricante, instalado no dispositivo do usuário deverá avaliar a postura do dispositivo, liberando ou não o acesso as aplicações baseando-se na identificação de itens, como:

1.9.1 Processo em execução;

1.9.2 Presença de arquivos armazenados em disco local;

1.9.3 Presença de um domínio Windows;

1.9.4 Presença de um certificado digital no dispositivo.

1.10. Deverá atuar como um roteador em nuvem, garantindo baixa latência e canal seguro, para aplicações privadas do MPBA;

1.11. Será permitida a inclusão de um appliance físico ou virtual na infraestrutura do MPBA para a comunicação segura entre nuvem do fabricante e servidores internos;

1.12. A solução deverá fornecer o acesso à aplicação apenas, não ao contexto de rede;

1.13. Deverá permitir o redirecionamento seguro para pelo menos 800 (oitocentas) aplicações internas;

1.14. Deverá ser capaz de autorizar o acesso ou não a aplicações internas baseada no perfil da máquina;

1.15. Deverá ser capaz de continuamente solicitar ao usuário que autentique novamente antes de ter acesso às aplicações privadas;

1.16. O acesso deve ser dedicado e exclusivo a aplicação designada na rede, não sendo permitido acesso irrestrito a um host ou a rede;

1.17. A solução de ZTNA deverá prover acesso seguro e controlado baseado nos protocolos TCP e UDP a aplicações privadas da MPBA através de cliente do próprio fabricante instalado na máquina;

1.18. A solução deverá suportar aplicações legadas baseadas em arquitetura cliente - servidor, operadas sob protocolos TCP/UDP.

1.19. Deverá prover acesso a pelo menos as seguintes aplicações:

1.19.1 SSH - TCP Porta 22;

1.19.2 HTTP - TCP Portas 80, 443 e Customizadas;

1.19.3 RDP - TCP 3389 e UDP 3389;

1.19.4 SQL Server - TCP 1333, 1434 | UDP 1434;

1.19.5 SMB - TCP 445;

1.19.6 FTP - TCP 21.

1.20. O acesso seguro as aplicações definidas poderão ser restritas, no mínimo, para:

1.20.1 Usuário Único;
1.20.2 Múltiplos Usuários;

1.20.3 Grupos de Usuário;

1.20.4 Unidade Organizacional (OU).

1.21. Para cada acesso, a política deverá prover múltiplas possibilidades de ações, dentre elas:

1.21.1 Permitir;

1.21.2 Bloquear.

1.22. Deve ser possível determinar apenas o endereço IP e porta de acesso da aplicação sem a necessidade de determinar um segmento de rede interno que o usuário remoto terá acesso;

1.23. Ao se conectar remotamente na solução para acesso a uma aplicação interna, a máquina remota não deve ter acesso, nem ser atribuído em um segmento de rede interna como em um sistema de VPN tradicional;

1.24. Deverá ser capaz de continuamente solicitar ao usuário que autentique novamente antes de ter acesso às aplicações privadas em um iDP externo (Microsoft azure AD).

1.25. A solução deverá prover o monitoramento de comportamento de usuário para identificar possíveis violações no acesso a aplicações web privadas.

1.26. A solução deverá suportar a importação de usuários a partir do Microsoft Active Directory.

1.27. A solução de segurança deverá suportar função Pre-Logon para plataformas Microsoft.

1.28. A solução deverá prover acesso a aplicações Web (HTTPS) sem a necessidade de instalação de agentes.

1.29. A solução deverá prover capacidade de avaliação contínua do endpoint para avaliação das validações de conformidade.

1.30. Deverá permitir o acesso diferenciado para um mesmo usuário conforme as seguintes condições:

1.30.1 Máquinas em conformidade: A partir de uma máquina gerenciada, com pré-requisitos de segurança identificados, deve permitir o acesso à aplicação.

1.30.2 Máquinas não conformes: A partir de uma máquina gerenciada, uma estação que não atenda aos requisitos de segurança, deve bloquear o acesso à aplicação.

1.31. CONSOLE DE GESTÃO CENTRALIZADA

1.32. A solução deverá possuir capacidade de gestão centralizada, mantendo um painel único de visibilidade para todos os módulos descritos neste termo de referência.

1.33. Toda a parte de gestão deverá ser centralizada em uma única console, garantindo a aplicação das políticas criadas em todos os pontos de presença disponíveis pelo fabricante e independente de qual data center o usuário faça uso, a política estará vigente para proteção e controle do tráfego.

1.34. Todos os dados disponíveis para a consulta e criação de relatórios, deverão residir na console de gestão por 90 dias.

1.35. A plataforma deve permitir a criação de diferentes perfis de acesso a console de administração com, no mínimo, as seguintes possibilidades:

1.35.1 Perfil de administrador geral: acesso total às funções da solução, acesso aos logs de auditoria dos outros usuários, criação e administração de outras contas de acesso;

1.35.2 Perfil de administrador intermediário: acesso total às funções da solução, exceto criação e administração de outras contas de acesso.

2.Item 2 – Serviços Gerenciados de Gestão de Exposição Cibernética por 36 meses

2.1 A solução deve realizar varreduras (scans) de vulnerabilidades, avaliação de configuração e conformidade (baseline e compliance);

2.2. A solução deve possuir recurso de varredura ativa, onde o scanner comunica-se com os alvos (ativos) através da rede;

2.3. A solução de gestão de vulnerabilidades deve suportar varreduras de dispositivos de IoT;

2.4. A solução deve ser licenciada pelo número de endereços IP ou dispositivos (assets);

2.5. A solução deve fornecer um modelo de armazenamento integrado que não dependa de um banco de dados externos ou de terceiros;

2.6. Caso a solução dependa de banco de dados de terceiros, todas as licenças deverão ser fornecidas pela **CONTRATADA**.

2.8. A solução deverá suportar API (Application Programming Interface) baseada em REST (Representatonal State Transfer) para automação de processos e integração com aplicações terceiras.

2.9 A solução deve possuir integração via API no mínimo as seguintes linguagens: Python, Powershell, Ruby, javascript, Java, Swift e PHP; A solução deve possuir métodos de consulta via api e envio, tais como: HTTP METHOD (POST, GET, PUT AND DELETE);

2.10. A solução deve incluir a opção para agentes instalados e licenciados em estações de trabalho e servidores, para varredura diretamente no sistema operacional;

2.11. Tais agentes devem ser gerenciados pela mesma interface/console da plataforma de gestão de vulnerabilidades;

2.12. A solução deve permitir o agrupamento de scanners para facilitar o gerenciamento e aplicação de políticas;

2.13. A solução deve realizar a varredura tanto de dispositivos na rede interna, dispositivos expostos a demais redes externas, tanto quanto dispositivos em nuvens públicas como Azure, AWS ou GCP;

2.14. O escaneamento para os dispositivos expostos deve sem realizados através de SCANS (ENGINE) do próprio fabricante alocados no Brasil;

2.15. Os scanners e sensores agentes deverão ser gerenciados por uma única plataforma, de maneira
centralizada;

2.16. O acesso a console de gerenciamento deve ser fornecida para pelo menos 10 usuários simultâneos;

2.17. A solução deve ser capaz de se integrar e disponibilizar insumos para soluções de correlação de eventos externa (SIEM);

2.18. A solução deve apresentar, para cada vulnerabilidade encontrada, a descrição e passos que devem ser tomados para correção;

2.19. A solução deve apresentar, para cada vulnerabilidade encontrada, evidências da vulnerabilidade através de saídas das verificações (outputs);

2.20. A solução deve fornecer controle de acesso baseado em função (RBAC- Role Based Access Control) para controlar o acesso do usuário a conjuntos de dados e funcionalidades;

2.21. A solução deve ser capaz de definir e gerenciar grupos de usuários, incluindo limitação de funções de varreduras e acesso a relatórios e dashboards;

2.22. A solução deve ter a capacidade de excluir determinados endereços IP do escopo de qualquer varredura ou scan;

2.23. A solução deve criptografar todos resultados de varreduras obtidos e informações inseridas tanto em descanso quanto em trânsito;

2.24. A solução deve suportar métodos de autenticação usando bases de autenticação local, e SAML (Security
Assertion Markup Language) para uso de SSO (Single SignOn);

2.25. A solução deve ser capaz de orquestrar scanners ilimitados dentro da infraestrutura;

2.26. A solução não deve impor nenhum limite de quantidade de scanners implementados dentro da infraestrutura;

2.27. A solução deverá possuir sistema de alertas para informar a disponibilidade de resultados dos escaneamentos através de email;

2.28. A solução deve oferecer capacidade de configuração dinâmica de grupos de ativos através de no mínimo as seguintes características:

2.29. Sistema Operacional, Endereço IP, DNS, NetBIOS Host, MAC, AWS Instance Type, AWS EC2 Name, Software instalado, Azure VM ID, AWS Region, Google Cloud Instance ID, Azure Resource ID, Ativos avaliados;
2.30. DOS RELATÓRIOS E PAINÉIS GERENCIAIS

2.31. A solução deverá possuir painéis gerenciais (dashboards) pré-definidos para rápida visualização dos resultados, permitindo ainda a criação de painéis personalizados;

2.32. Os painéis gerenciais deverão ser apresentados em diversos formatos, incluindo gráficos e tabelas, possibilitando a exibição de informações em diferentes níveis de detalhamento;

2.33. Os relatórios devem ser disponibilizados sob demanda no console de gerência da solução;

2.34. Os relatórios devem conter informações da vulnerabilidade, severidade, se existe um exploit disponível e informações do ativo;

2.35. A solução deve permitir a customização de dashboards/relatórios;

2.36. A solução deve concentrar todos os relatórios na plataforma central de gerenciamento, não sendo aceitas soluções fragmentadas;

2.37. A solução deve ser capaz de produzir relatórios, pelo menos, nos seguintes formatos: HTML, PDF e CSV;

2.38. A solução deve possibilitar a criação de relatórios baseado nos seguintes alvos: Todos os ativos e Alvos específicos;

2.39. Deve suportar a criação de relatórios criptografados (protegidos por senha configurável);

2.40. A solução deve suportar o envio automático de relatórios para destinatários específicos;

2.41. Deve ser possível definir a frequência na geração dos relatórios para no mínimo: Diário, Mensal, Semanal e Anual;

2.42. Permitir especificar níveis de permissão nos relatórios para usuários e grupos específicos;

2.43. DAS VARREDURAS

2.44. A solução deve realizar varreduras em uma variedade de sistemas operacionais, incluindo no mínimo Windows, Linux e Mac OS, bem como appliances virtuais;

2.45. A solução deve suportar varredura com e sem agente, de maneira ativa e passiva, distribuídas em diferentes localidades e regiões e gerenciar todos por uma console central;

2.46. A solução deve fornecer agentes instaláveis em sistemas operacionais distintos para monitoramento contínuo de vulnerabilidades;

2.47. Tais agentes devem realizar conexões para o sistema gerenciamento através de protocolo seguro;

2.48. A solução deve ser configurável para permitir a otimização das configurações de varredura;

2.49. A solução deve permitir a entrada e o armazenamento seguro de credenciais do usuário, incluindo contas locais, de domínio (LDAP e Active Directory) e root para sistemas Linux;

2.50. A solução deve fornecer a capacidade de escalar privilégios nos destinos, do acesso de usuário padrão até acesso de sistema ou administrativo;

2.51. A solução deve se integrar com solução de gerenciamento de acessos privilegiados para autenticação nos dispositivos, no mínimo, os seguintes:

2.52. CyberArk;

2.53. BeyondTrust;

2.54. Thycotic;

2.55. Centrify;

2.56. A solução deve suportar o agendamento de scans personalizados, incluindo a capacidade de executar varreduras em tempos designados, com frequência pré-determinada;

2.57. A solução deve ser capaz de identificar novos hosts no ambiente sem a necessidade de scan;

2.58. A solução deve possuir recurso de monitoria passiva do tráfego de rede para identificação de anomalias, novos dispositivos e desvios de padrões observados;

2.59. A solução deve ser capaz de realizar em tempo real a descoberta de vulnerabilidades nas seguintes tecnologias:
2.60. Cloud Services;

2.61. Data Leakage;

2.62. Database;

2.63. IoT;

2.64. Mobile Devices;

2.65. Operating System;

2.66. Peer-To-Peer;

2.67. SCADA;

2.68. Web Servers;

2.69. Web Clients;

2.70. A solução deve ser capaz de identificar a comunicação de malwares na rede de forma passiva;

2.71. A solução deve em tempo real, detectar logins e downloads de arquivos em um compartilhamento de rede;

2.72. DA ANÁLISE E PRIORIZAÇÃO DE VULNERABILIDADES

2.73. A solução deve ser capaz de exibir ambos severidade e pontuação, com base em CVSS (Common Vulnerability Scoring System) e inteligência de ameaças;

2.74. A solução deve utilizar sistema de pontuação e priorização das vulnerabilidades que utilize no mínimo:

2.75. CVSS Impact Score;

2.76. Idade da Vulnerabilidade;

2.77. Maturidade de códigos de exploração da vulnerabilidade encontrada;

2.78. Frequência de uso da vulnerabilidade em ataques e campanhas atuais;

2.79. Disponibilidade do código de exploração da vulnerabilidade;

2.80. Presença de módulos de exploração de vulnerabilidade em frameworks automatizados de exploração de vulnerabilidades como CANVAS, Metasploit e Core Impact;

2.81. Popularidade da vulnerabilidade em fóruns e comunicações na Darkweb;

2.82. O mecanismo de priorização deve ser sujeito a modificações e atualizações diárias com base em inteligência de ameaças e observação de tendências na Internet;

2.83. DA ANÁLISE DE RISCO DO AMBIENTE

2.84. A solução deve gerar um score que combine dados de vulnerabilidades com a criticidade dos ativos do ambiente computacional;

2.85. O score deve ser gerado automaticamente por meio de algoritmos de inteligência artificial (Machine
Learning) e deve calcular a probabilidade de exploração de uma determinada vulnerabilidade;

2.86. Deve ser capaz de calcular a criticidade dos ativos da organização;

2.87. A solução deve ser capaz de realizar um benchmark no ambiente do **CONTRATANTE** comparando sua maturidade com outras organizações do mesmo setor;

2.88. A solução deve prover visão sobre quais ações de remediação reduzem o maior nível de risco do ambiente;

2.89. A solução deve também permitir a visualização de ações de remediação agregadas para visão consolidada de redução de risco;

2.90. Deve permitir modificar a qualquer momento o tipo de indústria para comparação. Ex: Mudar de Setor Público para Mercado Financeiro;

2.91. Deve fornecer uma lista com as principais recomendações para o ambiente com foco na redução da exposição cibernética da organização;

2.92. A solução deve gerar uma pontuação para cada um dos ativos onde é levado em conta as vulnerabilidades presentes naquele ativo assim como a classificação do ativo na rede (peso do ativo);

2.93. A solução deve gerar uma pontuação global referente a exposição cibernética da organização baseado nas pontuações de cada um dos ativos;

2.94. A solução deve oferecer uma capacidade de comparação (benchmarking) da pontuação referente a exposição cibernética com outros players da mesma indústria assim como outras empresas do mercado;

2.95. A solução deve permitir um acompanhamento histórico do nível de exposição da organização;

2.96. Permitir realizar alterações na classificação dos ativos (atribuição de pesos diferentes) podendo sobrescrever a classificação atribuída automaticamente pela solução;

2.97. A solução deverá apresentar indicadores específicos referentes a remediação, possuindo no mínimo informações referentes ao tempo entre remediação e o tempo o qual a vulnerabilidade foi descoberta no ambiente, tempo entre a remediação e a data de publicação da vulnerabilidade, quantidade média de vulnerabilidades críticas por ativo e a comparação da quantidade de vulnerabilidades corrigidas por criticidade;

2.98. A solução deve permitir a segregação lógica entre áreas distintas da empresa afim de obter a pontuação referente exposição cibernética por área;

2.99. DO GERENCIAMENTO DA ANÁLISE DE ATAQUES EXPLORÁVEIS

2.100. Deve disponibilizar visibilidade nas técnicas de ataque baseado no framework MITRE ATT&CK;

2.101. Deve identificar qual a criticidade do ataque, em no mínimo: baixo, médio e alto;

2.102. Deve prover a evidência relacionada a descoberta do ataque;

2.103. Deve mostrar o objeto relacionado ao ataque, de origem e de destino;

2.104. Deve apresentar informações detalhadas relacionadas a mitigação para o ataque em análise;

2.105. Deve prover quais ferramentas e possíveis malwares associados ao ataque;
2.106. Deve disponibilizar de forma gráfica via console de gerenciamento as conexões entre os objetos do ataque;

2.107. Deve disponibilizar uma biblioteca com ‘Queries’ para a busca de objetos no mínimo os seguintes segmentos:

2.108. Rede;

2.109. Endpoint;

2.110. Active Directory;

2.111. Permissão;

2.112. Ransomware;

2.113. Vetores;

2.114. Credenciamento;

2.115. Deve suportar no mínimo 120 técnicas de ataques;

2.116. Deve possuir integração nativas com os módulos de WEB, Vulnerabilidades de Infraestrutura, Active Directory e ambientes em nuvem;

2.117. DA DESCOBERTA DE ATIVOS

2.118. A solução deve ser capaz de realizar escaneamento de descoberta de rede utilizando os seguintes critérios como alvo: IP, CIRD e Range;

2.119. A solução deve disponibilizar modelos de escaneamento de descoberta, ajustável, com os seguintes tipos de scan:

2.120. Enumeração de Hosts;

2.121. Identificação de Sistema Operacional (SO);

2.122. Port Scan (Portas comuns);

2.123. Port Scan (Todas as portas);

2.124. Customizado;

2.125. A solução deve permitir realizar escaneamento de descoberta customizado podendo ser parametrizado de acordo com a necessidade;

2.126. A parametrização do escaneamento de descoberta deve, no mínimo, conter os seguintes requisitos:

2.127. Descoberta de Host;

2.128. Ping o host remoto;

2.129. Usar descoberta rápida;

2.130. Métodos de ping;
2.131. ARP;

2.132. TCP;

2.133. ICMP;

2.134. UDP;

2.135. Escaneamento de descoberta de dispositivos de OT/SCADA;

2.136. Escaneamento de descoberta em redes de impressora;

2.137. Escaneamento em redes Novell;

2.138. Tecnologia de Wake-on-LAN;

2.139. Port Scanning:

2.140. Portas;

2.141. Considerar portas não escaneadas como fechadas;

2.142. Range de portas a serem escaneadas;

2.143. Enumerar Portas locais:

2.144. SSH (netstat);

2.145. WMI (netstat);

2.146. SNMP;

2.147. Descoberta de Serviços:

2.148. Sondar todas as portas para encontrar serviços;

2.149. Procurar por serviços baseado em SSL/TLS;

2.150. Enumerar todas as cifras SSL/TLS;

2.151. A solução deve realizar descoberta de ativo de forma passiva e adicionado automaticamente na console de gerenciamento;

2.152. A solução deve descobrir passivamente quando um host é adicionado na rede;

2.153. DA AVALIAÇÃO DE VULNERABILIDADE

2.154. A solução deve ser capaz de realizar testes sem a necessidade de agentes instalados no dispositivo destino para detecção de vulnerabilidades;

2.155. A solução deve detectar e classificar através de severidades, riscos e vulnerabilidades;

2.156. A solução deve também fornecer informações detalhadas sobre a natureza da vulnerabilidade, evidências da existência da vulnerabilidade e recomendações para mitigá-los;
2.157. A solução deve incluir uma saída detalhada das vulnerabilidades descobertas como versões de DLL esperadas e encontradas;

2.158. A solução deve ser compatível com CVE e fornecer pelo menos 10 anos de cobertura CVE;

2.159. A solução deve identificar vulnerabilidades especificas para o Active Directory com os seguintes padrões de verificação;

2.160. Contas administrativas vulneráveis a Kerberoasting attack;

2.161. Utilização de criptografia vulnerável com autenticação Kerberos;

2.162. Contas com pré-autenticação do Kerberos desabilitada;

2.163. Verificação de usuários com a opção de nunca expirar a senha com a opção habilitada;

2.164. Verificar validação de fragilidades do tipo “Unconstrained Delegation”;

2.165. Verificação de “Pre-Windows 2000 Compatible Access”;

2.166. Verificação de validade de chaves mestras "Kerberos KRBTGT”;

2.167. Verificação de “SID History Injection”;

2.168. Verificação de “Printer Bug Exploit”;

2.169. Verificação de “Primary Group ID”;

2.170. Verificação de usuários com Passwords em branco;

2.171. A solução deve suportar o uso de SMB e WMI para verificação de sistemas Microsoft Windows;

2.172. A solução deve ser capaz de iniciar automaticamente serviços de registro remoto em sistemas Windows ao executar uma varredura credenciada;

2.173. A solução deve ser capaz de parar automaticamente o serviço de registro remoto em sistemas Windows novamente assim que a varredura estiver completa;

2.174. O scanner deve oferecer suporte a shell seguro (SSH) com a capacidade de escalar privilégios para varredura de vulnerabilidades e auditorias de configuração em sistemas Unix;

2.175. A solução deve suportar o uso do netstat (Linux) e WMI (Windows) para uma enumeração rápida e precisa de portas em um sistema quando as credenciais são fornecidas;

2.176. A solução deve possibilitar a verificação remota de portas, além da enumeração local de portas, para ajudar a determinar se algum mecanismo de controle de acesso está sendo utilizado;

2.177. A solução deve fornecer auditoria de patch (MS Bulletins) para as principais versões de Windows;

2.178. A solução deve fornecer auditoria de patch para todos os principais sistemas operacionais Unix incluindo Mac OS, Linux, Solaris e IBM AIX;

2.179. A solução deve fornecer varredura para aplicativos comerciais diversos e proprietários, incluindo, mas não limitando-se a: Java, Adobe, Oracle, Apple, Microsoft, Check Point, Palo Alto Networks, Cisco, Fortinet, Fireeye, McAfee, etc;

2.180. A solução deve incluir classificação de severidades de acordo com o padrão Sistema Comum de Pontuação de Vulnerabilidade Versão (CVSS2 e CSVSS 3);

2.181. A solução deve fornecer informações acerca da disponibilidade de códigos de exploração das vulnerabilidades encontradas em frameworks de exploração para as plataformas mais populares: Core, Metasploit e Canvas;

2.182. A solução deve informar se a vulnerabilidade pode e está sendo ativamente explorada por código malicioso (malware);

2.183. A solução deve possuir importação de arquivos .YARA;

2.184. Deve ser capaz de identificar e classificar vulnerabilidades de máquinas virtuais em nuvem pública em infraestruturas como serviço nas plataformas AWS, Microsoft Azure e Google Cloud;

2.185. DA AUDITORIA DE CONFIGURAÇÃO

2.186. A solução deve ser capaz de realizar auditoria de conformidade sem a necessidade de agente instalado no dispositivo de destino;

2.187. A solução deve fornecer benchmarks de auditoria de segurança e configuração para conformidade regulatória e outros padrões de práticas recomendadas pela área ou fabricantes;

2.188. A solução deve realizar verificações de auditoria contendo as de segurança, com indicação de sucesso ou falha, baseado nos principais frameworks reconhecidos pela indústria, pelo menos os seguintes:

2.189. Center for Internet Security Benchmarks (CIS);

2.190. Defense Information Systems Agency (DISA) STIGs;

2.191. Health Insurance Portability and Accountability Act (HIPAA);

2.192. Payment Card Industry Data Security Standards (PCI DSS);

2.193. A solução deve fornecer auditoria de programas antivírus para determinação de presença e status de inicialização para no mínimo os seguintes produtos: TrendMicro Office Scan, McAfee VirusScan, Microsoft Endpoint Protection e Kaspersky;

2.194. A solução deve fornecer auditorias de configuração com base benchmarks em CIS (Center for Internet
Security) L1 e L2, para ambos os sistemas operacionais Microsoft Windows e Linux;

2.195. A solução deve permitir auditoria de conformidade em servidores Windows, Linux, Bancos de Dados SQL Server, a fim de determinar se estão configurados de acordo com os principais Framework de segurança como, por exemplo, CIS e DISA;

2.196. A solução deve oferecer validação e suporte a SCAP (Security Content Automation Protocol);

2.197. DA ANÁLISE DINÂMICA DE VULNERABILIDADES PARA APLICAÇÕES WEB

2.198. A solução deve ser capaz de analisar, testar e reportar falhas de segurança em aplicações Web como parte dos ativos a serem inspecionados;

2.199. A solução deve ser capaz de executar varreduras em sistemas web através de seus endereços IP ou FQDN (DNS);
2.200. A solução deve avaliar no mínimo os padrões de segurança OWASP Top 10 e PCI (payment card industry data security standard);

2.201. A solução deve suportar as diretivas PCI ASV 5.5 para definição de escopo de análise da aplicação;

2.202. A solução deve suportar as diretivas PCI ASV 6.1 para definição de balanceadores de carga das aplicações bem como suas configurações para inclusão no relatório de resultados;

2.203. A solução deve possuir templates prontos de varreduras entre simples e extensos;

2.204. Para varreduras extensas e detalhadas, deve varrer e auditar no mínimo os seguintes elementos:

2.205. Cookies, Headers, Formulários e Links;

2.206. Nomes e valores de parâmetros da aplicação;

2.207. Elementos JSON e XML;

2.208. Elementos DOM;

2.209. A solução deve permitir somente a execução da função crawler, que consiste na navegação para descoberta das URLs existentes na aplicação;

2.210. A solução deve ser capaz de utilizar scripts customizados de crawl com parâmetros definidos pelo usuário;

2.211. A solução deve excluir determinadas URLs da varredura através de expressões regulares;

2.212. A solução deve excluir determinados tipos de arquivos através de suas extensões;

2.213. A solução deve instituir no mínimo os seguintes limites:

2.214. Número máximo de URLs para crawl e navegação;

2.215. Número máximo de diretórios para varreduras;

2.216. Número máximo de elementos DOM;

2.217. Tamanho máximo de respostas;

2.218. Limite de requisições de redirecionamentos;

2.219. Tempo máximo para a varredura;

2.220. Número máximo de conexões HTTP ao servidor hospedando a aplicação Web;

2.221. Número máximo de requisições HTTP por segundo;

2.222. A solução deve detectar congestionamento de rede e limitar os seguintes aspectos da varredura:

2.223. Limite em segundos para timeout de requisições de rede;

2.224. Número máximo de timeouts antes que a varredura seja abortada;

2.225. A solução deve agendar a varredura e determinar sua frequência entre uma única vez, diária, semanal, mensal e anual;
2.226. A solução deve enviar notificações através de no mínimo E-mail e SMS;

2.227. A solução deve possuir a flexibilidade de selecionar quais testes serão realizados de forma granular, através da seleção de testes, plug-ins ou ataques;

2.228. A solução deve avaliar sistemas web utilizando protocolos HTTP e HTTPs;

2.229. A solução deve possibilitar a definição de atributos no cabeçalho (HEADER) da requisição HTTP de forma personalizado a ser enviada durante os testes;

2.230. A solução deve ser compatível com avaliação de web services REST e SOAP;

2.231. Deverá suportar no mínimo os seguintes esquemas de autenticação:

2.232. Autenticação básica (digest);

2.233. NTLM;

2.234. Form de login;

2.235. Autenticação de Cookies;

2.236. Autenticação através de Selenium;

2.237. Autenticação através de Bearer;

2.238. A solução deve importar scripts de autenticação selenium previamente configurados pelo usuário;

2.239. A solução deve customizar parâmetros Selenium como delay de exibição da página, delay de execução de comandos e delay de comandos para recepção de novos comandos;

2.240. A solução deve exibir os resultados das varreduras em tendência temporal para acompanhamento de correções e introdução de novas vulnerabilidades;

2.241. A solução deve exibir os resultados agregados de acordo com as categorias do OWASP Top 10 gory:OWASP_Top_Ten_Project); (https://www.owasp.org/index.php/Cate

2.242. Os resultados devem ser apresentados agregados por vulnerabilidades ou por aplicações;

2.243. Para cada vulnerabilidade encontrada, deve ser exibido evidências da mesma em seus detalhes;

2.244. Para vulnerabilidades de injeção de código (SQL, XSS, XSRF, etc.), deve evidenciar nos detalhes do evento encontrado:

2.245. Payload injetado;

2.246. Evidência em forma de resposta da aplicação;

2.247. Detalhes da requisição HTTP;

2.248. Detalhes da resposta HTTP;

2.249. Os detalhes das vulnerabilidades devem conter descrição da falha e referências didáticas para a revisão dos analistas;

2.250. Cada vulnerabilidade encontrada deve conter também soluções propostas para mitigação ou remediação das mesmas;

2.251. A solução deve possuir suporte a varreduras de componentes para no mínimo:

2.252. Wordpress, Blog Designer Plugin for Wordpress, Event Calendar Plugin for Wordpress, Convert Plus Plugin for Wordpress, AngularJS, Apache, Apache Tomcat, Apache Tomcat JK connecto, Apache Spark e Apache Struts, Atlassian Confluence, Atlassian Crowd e Atlassian Jira, Backbone.js, ASP.NET, Bootstrap, Drupal, Joomla!, jQuery, Lighttpd, Magento, Modernizr, Nginx, PHP, AJAX, Sitefinity, Telerik, ThinkPHP, Webmin e YUI;

2.253. DA ANÁLISE DE RISCO EM AMBIENTE MICROSOFT ACTIVE DIRECTORY

2.254. A solução deve identificar fraquezas ocultas em configurações do dedicadas ao Active Directory;

2.255. A solução deve possuir ações preventivas de hardening para o Active Directory;

2.256. A solução deve identificar ataque específicos para a estrutura do Active Directory;

2.257. A solução deve possuir funcionalidade para analisar em detalhes cada configuração incorreta que acarreta riscos de segurança – com uma linguagem simples, contextualizando tal risco para os times envolvidos;

2.258. A solução deve possuir recomendações de correção para cada configuração incorreta no Active Directory;

2.259. A solução deve avaliar relações de confiança perigosas entre florestas e domínios;

2.260. A solução deve capturar as mudanças que ocorrem no AD e demostrar na console de administração;

2.261. A solução deve possuir dashboard com os principais ataques e vulnerabilidades por domínio;

2.262. A solução deve permitir a correlação de mudanças no Active Directory e desvios de segurança;

2.263. A solução deve analisar em detalhes um ataque explorando as descrições através do framework MITRE ATT&CK;

2.264. A solução deve prover interface web para gerenciamento de todas as funcionalidades;

2.265. A solução deve possuir capacidade nativa de criação de dashboards customizados;

2.266. A solução deve suportar um modelo de controle de acesso baseado em funções (RBAC) flexível;

2.267. A solução deve realizar alterações no Active Directory, seus objetos e atributos;

2.268. A solução deve armazenar ou sincronizar nenhuma credencial de objetos do Active Directory;

2.269. A solução deve suportar ambientes com múltiplas florestas e domínios;

2.270. A solução deve suportar monitoramento contínuo de ambientes com Active Directory com o nível funcional de floresta e domínio a partir do 2003;

2.271. A solução deve suportar reter os eventos coletados por no mínimo um ano;

2.272. A solução deve descobrir e mapear a superfície de ataque do Active Directory e seus domínios monitorados com os seguintes padrões:

2.273. Não depender de agentes ou sensores para coleta de informações do AD;
2.274. A solução deve seguir as boas práticas de menor privilégio, a conta de serviço utilizada para conexão com o Active Directory, sendo o menor nível de acesso esperado para a conta de serviço como parte do grupo Domain User;

2.275. Interface web que consolida e apresenta de maneira unificada os domínios monitorados e as possíveis relações de confiança estabelecidas entre eles;

2.276. A solução deve analisar continuamente a postura de segurança do AD, minimamente avaliando:

2.277. Validação de GPOs desvinculadas, desabilitadas ou órfãs;

2.278. Validação de contas desativadas em grupos privilegiados;

2.279. Domínio usando uma configuração perigosa de compatibilidade com versões anteriores por meio de alterações no atributo dSHeuristics;

2.280. Validação de atributos relacionados a roaming de credenciais vulneráveis (ms-PKIDPAPIMasterKeys) gerenciados por um usuário sem privilégios;

2.281. Validação de domínio sem GPOs de proteção de computador, desativando protocolos vulneráveis antigos, como NTLMv1;

2.282. Validação de contas com senhas que nunca expiram;

2.283. Validação de senhas reversíveis em GPOs;

2.284. Validação de uso de senhas reversíveis em contas de usuário;

2.285. Validação de utilização de protocolo criptográfico fraco (Ex. DES) em contas de usuário; 2.286. Validação de uso do LAPS (Solução de senha de administrador local) para gerenciar senhas de contas locais com privilégios;

2.287. Validação se o domínio possui um nível funcional desatualizado; 2.288. Validação de contas de usuário utilizando senha antiga;

2.289. Validação se o atributo AdminCount está definido em usuários padrão;

2.290. Validação do uso recente da conta de administrador padrão;

2.291. Validação de usuários com permissão para ingressar computadores no domínio;

2.292. Validação de contas dormentes;

2.293. Validação de computadores executando um sistema operacional obsoleto;

2.294. Validação de restrições de logon para usuários privilegiados em ambiente com múltiplos tiers (1, 2 e 3) de segregação de ativos;

2.295. Validação de direitos perigosos configurados no Schema do AD;

2.296. Validação de relação de confiança perigosa com outras Florestas e Domínios;

2.297. Validação de contas que possuem um atributo perigoso de histórico SID (SID History);

2.298. Validação de contas utilizando controle de acesso compatível com versões anteriores ao Windows 2000;

2.299. Validação da última alteração de senha do KDC;

2.300. Validação da última alteração da senha da conta SSO do Azure AD;

2.301. Validação de contas que podem ter senha em branco/vazia;

2.302. Validação de utilização do grupo nativo Protected Users;

2.303. Validação de privilégios sensíveis (Ex. Debug a program, Replace a process level token, etc.) perigosos atribuídos aos usuários;

2.304. Validação de possível senha em clear-text;

2.305. Validação de sanidade das GPOs e componentes CSEs (Client-Side Extension);

2.306. Validação de uso de algoritmos de criptografia fracos na PKI do Active Directory;

2.307. Validação de contas de serviço com SPN (Service Principal Name) que fazem parte de grupos privilegiados;

2.308. Validação de contas anormais nos grupos administrativos padrão do AD;

2.309. Validação de consistência no container adminSDHolder;

2.310. Validação de delegação Kerberos perigosa;

2.311. Validação em permissões de objetos raiz que permitem ataques do tipo DCSync;

2.312. Validação de políticas de senha fracas aplicadas aos usuários; 2.313. Validação das permissões relacionadas às contas do Azure AD Connect;

2.314. Validação do ID do grupo primário do usuário (Primary Group ID);

2.315. Validação de permissões em GPOs sensíveis associadas aos Containers Configuration, Sites, Root Partition e OUs sensíveis como Domain Controllers;

2.316. Controladores de domínio gerenciados por usuários ilegítimos;

2.317. Validação de certificado mapeado através de atributo altSecurityIdentities em contas privilegiadas;

2.318. Validação de uso de protocolo Netlogon inseguro (Zerologon/CVE-2020-1472);

2.319. A solução deve identificar vulnerabilidades e configurações incorretas do AD à medida que são introduzidas sendo:

2.320. Identificar todas as vulnerabilidades e configurações incorretas no AD;

2.321. Monitorar relações de confiança perigosas em toda a estrutura AD;

2.322. Apresentar ameaças e alterações sem a necessidade de scans estáticos e programados no Active Directory e sua infraestrutura;

2.323. Apresentar as ameaças e alterações em tempo real ou em menos de cinco minutos;

2.324. DETECÇÃO DE ATAQUES AO AD EM TEMPO REAL:

2.325. Monitorar continuamente os indicadores de possíveis ataque como DCSync, DCShadow, Password Spraying, Password Guessing/Brute Force, Lsaas Injecton nos

controladores de domínio, Golden Ticket, NTLM Relay, entre outros;

2.326. Detecção de ataques ao AD em tempo real ou em menos de um minuto;

2.327. Análise detalhada do ataque, apresentando ativo de origem, vetor de ataque, controlador de domínio afetado, técnica aplicada;

2.328. Apresentação de ataques em uma linha do tempo;

2.329. Investigar ameaças, reproduzir ataques e procurar por backdoors;

2.330. Permitir busca ágil de eventos específicos na base da solução através de queries customizadas;

2.331. A solução deve ser capaz de enviar alertas por e-mail;

2.332. A solução nativamente deve ser capaz de se integrar com SIEM através de protocolo SYSLOG;

2.333. A solução deve ser capaz de filtrar e enriquecer os eventos que serão enviados para o SIEM;

2.334. A solução deve produzir regras YARA na detecção de ataques (Ex. DCSync, Golden Ticket) identificados pela ferramenta;

2.335. A solução deve possuir conjunto de APIs REST, todas as chamadas disponíveis devem estar contidas na documentação;

2.336. A solução deve permitir a criação de listas de exclusões, suportando minimamente Exclusão por domínios do AD monitorados e por itens analisados;

2.337. A solução deve ser licenciada pelo número de usuários habilitados;

2.338. DO GERENCIAMENTO DA SUPERFÍCIE DE ATAQUE

2.339. Deve avaliar a superfície de ataque externo, apresentando como a organização e seus ativos expostos na Internet são vistos pelos atacantes e quais as vulnerabilidades encontradas.

2.340. Deve identificar ativos usando registros DNS, endereços IP e ASN.

2.341. Deve possuir mecanismo de busca personalizada em base em filtros customizados.

2.342. Deve permitir exportação de dados nos seguintes padrões:

2.343. CSV

2.344. JSON

2.345. XLSX

2.346. Deve avaliar a postura de segurança de toda a sua superfície de ataque externo incluindo entradas de filtro do tipo:

2.347. Screenshot da aplicação web.

2.348. Tags personalizadas
2.349. Networking

2.350. IP

2.351. ASN 2.352. CDN

2.353. SaaS

2.354. PaaS

2.355. IaaS

2.356. Remote Access

2.357. Host

2.358. Domain

2.359. Proxy Reverso

2.360. Tipo de serviços

2.361. SSL/TLS

2.362. SSL / TLS Expiration

2.363. SSL / TLS Fingerprint

2.364. SSL / TLS Cypher Suites

2.365. SSL / TLS protocol

2.366. SSL / TLS error

2.367. SSL / TLS Serial Number

2.368. Cookie compliance

2.369. RBL

2.370. Localização

2.371. País

2.372. Cidade

2.373. Latitude

2.374. Longitude

2.375. Time Zone

2.376. Web applications

2.377. Redes Sociais
2.378. HTTP response

2.379. HTTP headers

2.380. HTTP Security headers

2.381. Whois

2.382. Estrutura de Marketing como:

2.383. Google Analytics

2.384. Google Adsense

2.385. CRM 2

.386. SEO

2.387. Media

2.388. Webcams

2.389. Printers

2.390. Video Players

2.391. Media Servers

2.392. Deve sugerir domínios a serem analisados com base nas entradas de registro inicialmente analisados.

2.393. Deve possuir integração com ServiceNow e Slack para notificações automáticas.

2.394. Deve possuir um dashboard com interação gráfica via web, para acompanhamento das vulnerabilidades encontradas.

3. Item 3 – Serviço Gerenciados de visibilidade, conformidade, segurança e orquestração dos dispositivos conectados à rede corporativa por 36 meses.

3.1. Características Gerais

3.2. A solução deverá ser fornecida e formato de appliances virtuais;

3.3. O fornecimento deve contemplar solução gerenciamento central de múltiplos appliances virtuais, bem como integração com soluções de terceiros a partir de protocolos abertos, tais como SQL, LDAP e Web Services;

3.4. As licenças poderão ser distribuídas em múltiplos appliances virtuais, gerenciados centralmente, em unidades de 1000 licenças, conforme a necessidade do **CONTRATANTE**;

3.5. Não poderá haver limitação no número de appliances virtuais gerenciados;

3.6. A solução deverá ser fornecida em formato de appliance virtual compatível com o VMware ESXi, Microsoft
HyperV e Linux KVM, podendo ser utilizados on-premises e, também, em nuvem pública AWS e Azure;

3.7. Deve monitorar todo o tráfego da rede através de uma porta espelhada no switch core (porta SPAN);

3.8. Deve realizar todas as suas funções sem a utilização de agentes (AGENTLESS) instalados nas máquinas corporativas (estações de trabalho, servidores, dentre outros);

3.9. Deve criar e manter atualizada, em tempo real, a lista de todos os elementos da rede, incluindo equipamentos de rede, impressoras, dispositivos de usuários finais, servidores, sistemas operacionais, aplicações, processos, portas abertas, dispositivos periféricos, vulnerabilidades e usuários, permitindo o agrupamento automático baseado em condições, e a aplicação automática de ações de controle de acesso, garantia de conformidade (remediação) e orquestração de segurança;

3.10. Deve ser capaz de classificar automaticamente impressoras, dispositivos de rede, máquinas Windows,
Linux e Macintosh, Dispositivos Móveis e dispositivos que estejam realizando tradução de endereços (NAT);

3.11. Deve ser capaz de diferenciar máquinas corporativas de máquinas não corporativas;

3.12. Deve ser capaz de classificar os dispositivos de IT (Information Technology) e OT (Operational Technology) por função em subcategorias, no mínimo:

3.13. IT: Computador, Mobile, Networking, Storage, Acessórios (ex: impressoras);

3.14. OT: Sistema de Aquisição de Dados, Monitoramento Ambiental, Sistema de Controle Industrial, Segurança Física (ex: Cameras IP), Monitoramento e Controle Remoto, Saúde.

3.15. Deve ser capaz de classificar dispositivos por sistema operacional contendo, no mínimo as seguintes categorias: Alcatel-Lucent, Android, Avaya, Chrome OS, Cisco IOS, Cisco ASA-OS, Cisco Access Points, ExtremeXOS, FortiOS, Huawei VRP, iOS, LG Web OS, Linux, Macintosh, UNIX, Windows;

3.16. Deve ser capaz de classificar dispositivos por fabricante e modelo para dispositivos IoT (Internet of Things), tais como wearables e dispositivos móveis, e OT (Operational Technology), tais como sistemas de controle industrial;

3.17. Deve ser capaz de realizar a classificação passiva de dispositivos para que a classificação seja realizada sem contato ativo direto com o dispositivo (ex: para dispositivos que controlam processos operacionais de tempo real);

3.18. Deve ser capaz de criar inventário das informações da rede e dos dispositivos catalogando, pelo menos, sistemas operacionais e respectivas versões, máquinas e respectivas versões dos sistemas operacionais Windows, Linux e Mac, processos em execução (Windows, Linux e Mac), portas de comunicação abertas nos dispositivos, aplicações instaladas em Windows, dispositivos externos conectados, usuários registrados como visitantes, dentre outras;

3.19. Deve permitir o controle de acesso à rede baseado em perfis e regras de conformidade;

3.20. Deve prover funções de visibilidade e controle para ambientes de nuvem nas seguintes plataformas: AWS,
Azure, VMWare vCenter, VMWare NSX e VMWare vSphere;

3.21. Deve possuir autenticação de usuários com LDAP, RADIUS, Active Directory e 802.1x, possuindo, ainda, um servidor RADIUS e RADIUS Proxy integrado para facilitar o deployment baseado em 802.1x;

3.22. Deve suportar segurança 802.1x pre-connect e controle 802.1x post-connect tanto para rede cabeada como rede sem fio tanto de usuários corporativos como visitantes;

3.23. Deve suportar RADIUS authentication, authorization e accounting;

3.24. Deve possuir catálogo de MAC Addresses para suportar Mac Address Bypass para dispositivos que não suportam 802.1x;
3.25. Deve permitir que a autenticação 802.1x seja realizada através de servidor Microsoft Active Directory e servidor RADIUS externo (RADIUS Proxy);

3.26. Deve ser capaz de atribuir labels aos dispositivos baseados em listas de MAC Addresses mantidos em servidores FTP ou LDAP;

3.27. Deve permitir a automação do registro de convidados, tanto na rede cabeada como na rede sem fio, através de captive portal, sem necessidade de configuração/reconfiguração de equipamentos de acesso (switches);

3.28. Deve identificar automaticamente os servidores de DNS da rede;

3.29. Deve garantir a conformidade das configurações das máquinas corporativas (estações de trabalho, servidores, dispositivos móveis, dentre outros) com as políticas de segurança da organização, incluindo controle das soluções baseadas em agentes, tais como antivírus, patches de sistema operacional e bloqueio de software não-autorizado;

3.30. Deve realizar a detecção de ameaças baseada em análise do comportamento dos dispositivos (pósadmissão) não baseada em assinaturas (ex: Port Scan (TCP/UDP), Ping Sweep Scan, SNMP Scan, User Scan, Tentativa de Infecção via rede) e permitir o monitoramento e bloqueio do dispositivo;

3.31. Deve detectar dispositivos não-autorizados, tais como switches e access points (APs), identificando ainda se é um dispositivo que realiza tradução de endereços (NAT) e se está ou não autorizado a utilizar a rede;

3.32. Deve detectar portas de switches com múltiplos hosts conectados;

3.33. Deve detectar dispositivos sem endereço IP (tais como stealthy packet capture devices projetados para furto de informações) e executar ações de bloqueio de porta do switch e mudança de VLAN;

3.34. Deve controlar os dispositivos móveis conectados à rede em tempo real;

3.35. Deve possuir inventário e controle da rede em tempo real, permitindo rastrear e controlar usuários, aplicações, processos, portas e dispositivos externos;

3.36. Deve ser capaz de definir segmentos de rede baseados em endereços IP e filtrar os dados apresentados baseados em segmentos;

3.37. Deve permitir a criação de subsegmentos para diferenciar os setores e poder aplicar as políticas em diferentes segmentos;

3.38. Deve ser capaz de definir unidades organizacionais baseadas em segmentos de rede e filtrar os dados baseados em unidades organizacionais;

3.39. Deve ser capaz de realizar avaliação de postura de segurança de dispositivos IoT (Internet of Things) através da avaliação do uso de credenciais (SNMP, SSH e Telnet):

3.40. Padrão/Default de fábrica;

3.41. Base do fabricante de credenciais fracas/comuns;

3.42. Credenciais fornecidas manualmente pelo administrador.

3.43. Deve possuir módulo de relatórios e dashboard para monitoramento do nível de conformidade (compliance);

3.44. Deve possuir mecanismo para scanear máquinas Windows em busca de IOC's (Indicators of Compromise) e executar ações em resposta à identificação de máquinas comprometidas;

3.45. Cada IoC deverá poder ser composto, pelo menos, dos seguintes atributos: Nome da Ameaça, Nome do Arquivo, Tamanho do Arquivo, Hash do Arquivo, Tipo de Função Hash Utilizada, Severidade, Endereço de Central de Comando & Controle (CnC);

3.46. Deve possuir mecanismo automático de remoção de IoC's da base de dados da solução de acordo com a severidade e tempo de existência do IoC;

3.47. Deve permitir a automação e orquestração de soluções de terceiros a partir de eventos detectados pela solução, utilizando-se das capacidades de integração em ações definidas nas políticas da solução;

3.48. As ações devem poder ser encadeadas através de agendamento da sua execução permitindo a orquestração de resposta a incidentes através de comunicação com soluções de terceiros via protocolos abertos (LDAP, SQL e Web Services);

3.49. Deve ser capaz de detectar novos dispositivos de rede a partir de traps SNMP v1, v2c e v3 enviados pelos switches;

3.50. Deve ser capaz de executar ações e consultar informações em switches de diversos fabricantes e switches genéricos através de protocolo SNMP;

3.51. Deve suportar SNMP v1, v2c e v3 para permitir o monitoramento do appliance através de sistemas externos de monitoramento de rede;

3.52. Deve ser capaz de enviar traps SNMP para sistemas de monitoramento de rede quando ocorrerem modificações de configuração e quando os limites de utilização do sistema forem ultrapassados (ex: número de dispositivos gerenciados, utilização de CPU, utilização de memória, perda de pacotes etc.);

3.53. Deve ser capaz de enviar e receber mensagens via SYSLOG;

3.54. Deve ser capaz de usar informações do tráfego DHCP para classificar os dispositivos sem a necessidade de utilização de IP Helper Address para redirecionamento das requisições DHCP;

3.55. Deve ser capaz de analisar o tráfego de rede e calcular estatísticas como tamanho médio de pacote, número médio de pacotes por segundo e resoluções de nomes via DNS;

3.56. Deve ser capaz de receber e processar informações de Flow (NetFlow v9, IPFIX e sFlow) para identificação de dispositivos e propriedades de dispositivos;

3.57. Deve ser capaz de identificar, aplicar políticas, manter a segurança e garantir a conformidade de dispositivos na nuvem pública da Amazon – AWS, inclusive identificando e controlando instâncias Elastic Compute Cloud (EC2), usuários Identity and Access Management (IAM) e Virtual Private Clouds (VPCs), permitindo:

3.58. Ver instâncias EC2, usuários IAM e VPCs;

3.59. Criar e aplicar políticas nestas entidades AWS;

3.60. Manter a segurança e conformidade das instâncias de nuvem, usuários IAM e VPCs.

3.61. Deve ser capaz de identificar, aplicar políticas, manter a segurança e garantir a conformidade de dispositivos na nuvem pública da Microsoft – Azure, inclusive identificando e controlando instâncias de Virtual Machines (VM) e Virtual Networks (VNET), permitindo:
3.62. Ver instâncias VM e redes VNETs;

3.63. Criar e aplicar políticas nestas entidades Azure;

3.64. Manter a segurança e conformidade das instâncias de VM's e VNET's.

3.65. Deve suportar a descoberta e gerenciamento de dispositivos em máquinas virtuais VMWare vSphere/vCenter;

3.66. Deve ser capaz de aplicar funcionalidades de controle em máquinas virtuais de ambientes VMWare vSphere/vCenter; 3.67. Desligar máquina virtual;

3.68. Ligar máquina virtual;

3.69. Reiniciar máquina virtual;

3.70. Colocar a máquina em espera;

3.71. Instalar e atualizar VMware Tools;

3.72. Desconectar todas as placas de redes da máquina virtual;

3.73. Alterar o Virtual Port Group da máquina virtual. 3.74. Deve ser capaz de aplicar microssegmentação em máquinas virtuais de ambientes VMWare NSX; 3.75. Deve ser capaz de identificar dispositivos e servidores configurados com o uso de credenciais comuns da empresa e que devem ser considerados inseguros;

3.76. Deve possuir trilha de auditoria acessível pela interface gráfica que registre todas as operações de modificação nas configurações da solução (adições, edições e remoções).

3.77. ATRIBUTOS E PROPRIEDADES

3.78. Deve ser capaz de identificar atributos e propriedades dos dispositivos para permitir a criação de políticas baseadas em condições, no mínimo:

3.79. Autenticação: Identificar autenticação via HTTP (80/TCP), Telnet(23/TCP), NetBIOS(139/TCP), FTP(21/TCP)
IMAP (143/TCP), POP3(110/TCP), rlogin(513/TCP) e Active Directory;

3.80. Dispositivo: banners de serviço, endereço IP, nome DNS, se está realizando NAT, usuário logado, interfaces de rede, resultados de scripts, portas abertas, número de endereços IPv4 e IPv6, NIC Vendor, NetBIOS Hostname, NetBIOS Domain, qualquer atributo SNMP do dispositivo, resultado de comando via SSH;

3.81. Usuário: nome, status da autenticação e grupo de trabalho;

3.82. Windows Active Directory: conta desabilitada, conta expirada, Display Name, Member Of, Email, Initials,
etc;

3.83. Sistema Operacional (Windows/Linux/Mac): tipo e versão do SO; processos em execução; existência, data e tamanho de arquivos; resultado de execução de scripts, usuário logado;

3.84. Detalhes de Máquinas Windows: domínio, último evento de login, existência e valores de chaves de registro, serviços instalados, serviços em execução, vulnerabilidades, dispositivos externos;

3.85. Detalhes de máquinas virtuais: Health Status de máquinas Guest VMWARE e tipo de instância Amazon EC2;

3.86. Segurança: agente de antivírus instalado, nível de atualização e status de firewall, IoC's (Indicators of Compromise), ARP Spoofing, sessões abertas como cliente, sessões abertas como servidor, traps SNMP recebidas da porta onde o dispositivo está conectado;

3.87. Aplicações Windows: aplicações instaladas, incluindo versão, aplicações de Cloud Storage, Instant Messaging, Criptografia de Disco e Peer to Peer instaladas e em execução;

3.88. Periféricos: tipo do dispositivo, fabricante e tipo de conexão;

3.89. Rede: segmento de rede, switch e porta ao qual o dispositivo está conectado, VLAN.

3.90. Deve ser capaz de criar novas propriedades/atributos para os dispositivos usando o resultado de scripts executados nos dispositivos (ex: quantidade de instâncias de um determinado processo em execução em servidores Linux);

3.91. Deve ser capaz de criar novas propriedades/atributos para os dispositivos baseado em valores consultados em bases de dados externas via SQL, Web Services e LDAP;

3.92. Deve ser capaz de criar novas propriedades baseado na comparação entre propriedades já existentes;

3.93. Deve ser possível criar listas de valores de propriedades para serem usadas como operandos em regras de políticas (Ex: Listas de Endereços IP, Listas de Nomes de Máquinas, Listas de Processos, etc);

3.94. Deve ser possível detectar mudanças de valores em propriedades tais como: aplicações Windows instaladas e/ou removidas, novas interfaces de rede, mudança de data, tamanho e versão de arquivos Windows, criação/remoção de arquivos Windows, mudança de endereço IP, mudança de nome no DNS, alterações no Windows Registry, mudança de porta no switch, dentre outras, e utilizá-las como condições nas regras das políticas para execução de ações;

3.95. Deve ser possível utilizar atributos e propriedades para organizar os dispositivos em grupos, de forma a permitir melhor controle sobre a aplicação de políticas.

3.96. AÇÕES

3.97. Deve ser possível definir os seguintes tipos de ações automáticas nas políticas:

3.98. Restringir o acesso através de modificação de VLAN, desabilitar porta de switch e TCP Resets (Firewall Virtual);

3.99. As ações de Firewall Virtual (TCP Resets) devem poder ser realizadas no tráfego originado pelo dispositivo e no tráfego destinado ao dispositivo; 3.100. Bloquear acesso de e para hosts e portas específicas;

3.101. Deve ser possível especificar o segmento de rede/faixa de IP e portas que estão impedidos de se comunicar com o dispositivo bloqueado;

3.102. Deve ser possível criar exceções à regra para permitir o acesso de administradores ao dispositivo;

3.103. A solução deve realizar ação de Virtual Firewall sem modificação na infraestrutura utilizando, apenas, informações coletadas no espelhamento de porta (Port SPAN).

3.104. Notificar o usuário através de redirecionamento de tráfego HTTP a partir da escuta do tráfego espelhado (SPAN port), inclusive em ambientes que utilizam Web Proxy;

3.105. Deve ser possível redirecionar o tráfego para qualquer URL definida pelo administrador;

3.106. Deve ser possível criar exceções para impedir o redirecionamento de tráfego direcionado a URL's específicas;

3.107. Deve ser possível criar exceções para impedir o redirecionamento de tráfego para segmentos de rede e faixas de IP específicas;

3.108. A solução deve realizar ação de redirecionamento de tráfego HTTP sem modificação na infraestrutura utilizando, apenas, informações coletadas no espelhamento de porta (Port SPAN).

3.109. Redirecionar tráfego usando HTTPS;

3.110. Bloquear tráfego HTTPS passando através de servidor Proxy;

3.111. Permitir redirecionar os usuários para páginas de autenticação e de ações de remediação;

3.112. A solução deve realizar ação de redirecionar os usuários para página de autenticação sem modificação na infraestrutura utilizando, apenas, informações coletadas no espelhamento de porta (Port SPAN)

3.113. Permitir definir exceções para URL's específicas;

3.114. Registrar convidados através de formulário de registro (captive portal) para máquinas não corporativas (terceiros, visitantes, BYOD), tanto para acessos via rede cabeada como rede sem fio, sem necessidade de configuração/reconfiguração de equipamentos de acesso (ex: switches), com as seguintes capacidades:

3.115. Permitir definir a validade de tempo de acesso do usuário;

3.116. Capacidade de definir diversos tipos de convidados com privilégios diferenciados;

3.117. Atribuir limitações de rede de acordo com o usuário;

3.118. Formulário de auto registro com acesso automático, sem necessidade de aprovação;

3.119. Formulário de auto registro com envio de códigos de verificação via e-mail para permitir o acesso (one time password);

3.120. Formulário de auto registro com aprovação de acesso por "sponsor" devidamente autorizado

3.121. Controlar o acesso do convidado até que o seu acesso seja aprovado pelo "sponsor" indicado;

3.122. Possuir Dissovable Agent para levantamento de informações e aplicação de políticas de conformidade em máquinas não corporativas, sem necessidade de permissões de administrador para execução e sem processo de instalação, não deixando nenhum rastro após o reboot.

3.123. Redirecionamento de tráfego via DNS (DNS Enforcement);

3.124. Comunicação: enviar e-mail de alertas aos usuários e administradores, notificar de usuário através de redirecionamento HTTP, enviar traps SNMP, envio de registros para SYSLOG;

3.125. Remediação de sistema operacional Windows: instalar patch de sistema operacional; criar e modificar chaves de registro; iniciar agente de segurança e atualizar assinaturas; desabilitar dispositivo externo, encerrar processos de Cloud Storage, P2P e IM;

3.126. Iniciar e encerrar processos e scripts em Windows, Linux e Mac;

3.127. Executar scripts no dispositivo com passagem de parâmetros para o script com valores dos atributos disponíveis sobre o dispositivo;

3.128. Deve ser possível executar scripts como “root” em dispositivos Linux usando “sudo”.

3.129. Executar scripts no servidor da solução com passagem de parâmetros para o script com valores de atributos disponíveis do dispositivo;

3.130. Bloquear tráfego malicioso e colocar em quarentena dispositivo malicioso;

3.131. Atribuir dispositivos a grupos para utilização como critério de filtragem em políticas;

3.132. Enviar comandos para soluções de terceiros, através de protocolo aberto (SQL, LDAP e Web Services);

3.133. Iniciar atualizações de segurança do Windows, via Microsoft Web site ou WSUS;

3.134. Deve permitir escolher um dos três métodos de atualização disponíveis na plataforma: download e instalação automáticas, download automático e notificação do usuário, usando as configurações de “automatic update” do dispositivo.

3.135. A solução deve ser fornecida com plugin específico de integração com a solução de gestão de vulnerabilidades ofertada pela CONTRATADA;

3.136. Deve possuir um assistente, via WEB, que permita aos próprios usuários aplicarem ações de remediação de vulnerabilidades do sistema operacional Windows que tenham sido detectadas no dispositivo;

3.137. Todas as ações executadas sobre um dispositivo devem ser registradas (log) nas informações detalhadas do dispositivo.

3.138. POLÍTICAS

3.139. As políticas devem ser compostas por regras de condição e execução de ações em um escopo específico;

3.140. Deve permitir a limitação de escopo de aplicação da política baseado em faixas de endereço IP, segmentos de rede e grupos de dispositivos;

3.141. Deve permitir criar exceções para escopo de políticas baseado em endereço IP, MAC Address, NetBIOS Hostname; Username e grupos de dispositivos;

3.142. As regras de cada política devem ser criadas com base em condições lógicas (AND, OR, NOT) sobre quaisquer propriedades/atributos e informações levantadas sobre cada dispositivo;

3.143. Deve ser possível definir se o resultado da avaliação de uma condição será verdadeiro ou falso em caso de ausência de informações sobre a propriedade/atributo que está sendo avaliado;

3.144. Cada regra deve suportar a execução de múltiplas ações e o agendamento das mesmas para permitir flexibilidade na implementação de ações de controle de acesso, remediação e orquestração de segurança;

3.145. O agendamento de ações deve suportar pelo menos as seguintes opções:

3.146. Imediatamente;

3.147. Após um intervalo de tempo definido pelo administrador;

3.148. Data e hora específica. 3.149. Deve ser possível estabelecer a duração da aplicação das ações com as seguintes opções:

3.150. Sem data final;

3.151. Após um intervalo de tempo definido pelo administrador;

3.152. Data e hora específica.

3.153. Deve ser possível atribuir labels aos dispositivos e criar contadores para implementar lógicas de políticas complexas, capazes de reter o estado do dispositivo durante os processos de reverificação das condições lógicas;

3.154. Deve permitir a criação de um catálogo de condições customizadas para serem reutilizadas em regras de diferentes políticas;

3.155. Deve ser possível definir novas propriedades do dispositivo baseado na comparação ente outras propriedades já existentes;

3.156. As políticas criadas pelo administrador deverão permitir estabelecer condições de classificação e conformidade (compliance) de dispositivos, bem como definir ações automáticas de remediação, tais como:

3.157. Identificar hosts e colocar em quarentena quando não houver o software de antivírus instalado ou não estiver com os patches de sistema atualizados;

3.158. Limitar acesso à rede para convidados;

3.159. Ativar detecção automática para hosts que estão faltando service pack e integrar com ferramenta de correção (WSUS);

3.160. Verificar todos os servidores que não estão em conformidade (compliance) com as políticas;

3.161. Automaticamente deverá descobrir e colocar em quarentena os access points (APs) wireless desconhecidos.

3.162. Deve possuir capacidade de atualizar bases de dados externas via comandos SQL parametrizados com dados dos dispositivos disponíveis na solução;

3.163. Deve ser capaz de executar comandos em soluções de terceiros através de chamadas de Web Services parametrizados com dados dos dispositivos disponíveis na solução;

3.164. Deve possuir capacidade de buscar informações em soluções de terceiros, através de LDAP, SQL e Web
Services, para aplicação de políticas de segurança, controle de acesso e conformidade de dispositivos;

3.165. Deve possibilitar a importação e exportação de políticas;

3.166. Deve fornecer as informações sobre os dispositivos em tempo real;

3.167. Deve possuir templates de políticas pré-definidas e assistente gráfico para permitir a criação rápida de políticas padrão;

3.168. Deve permitir detectar usuários e dispositivos que estão fora de conformidade com a política de segurança, informando na console a razão da não-conformidade e detalhes completos do usuário/dispositivo, permitindo ainda a aplicação de ações automáticas de remediação;

3.169. Deve executar envio de alertas, restrições de acesso e ações de remediação automáticas, incluindo:
3.170. Atribuição de um dispositivo a VLANs específicas para controle de acesso;

3.171. Migração do dispositivo automaticamente para rede de convidados;

3.172. Migração de um dispositivo da rede de produção para uma rede de quarentena;

3.173. Finalização de aplicações não-autorizadas nas estações de trabalho e servidores corporativos.

3.174. INVENTÁRIO EM TEMPO REAL

3.175. Deve possuir inventário de usuários, dispositivos, software, hardware e rede com, no mínimo, as seguintes categorias:

3.176. Inventário de usuários da rede;

3.177. Inventário de convidados registrados incluindo status da aprovação de acesso, identificação do aprovador e da pessoa de contato indicada durante o processo de registro;

3.178. Inventário de portas de comunicação abertas associadas aos respectivos dispositivos;

3.179. Inventário de vulnerabilidades Microsoft associadas aos respectivos dispositivos;

3.180. Inventário de hardware de máquinas Windows contendo:

3.181. Informações gerais do equipamento: número de processadores, total de memória física, fabricante, modelo, time zone;

3.182. Discos: tipo do drive, nome do volume, tamanho, espaço disponível;

3.183. Monitores: tipo e fabricante; 3.184. Placa mãe: fabricante e modelo;

3.185. Adaptadores de rede: índice, endereço MAC, endereço IP, subrede IP e default gateway;

3.186. Memória física: capacidade, tipo, velocidade e fabricante;

3.187. Dispositivos Plug-and-Play: Class GUID, Device ID e fabricante;

3.188. Processador: fabricante, arquitetura, família, max clock speed, número de cores, percentual de carga e status.

3.189. Inventário de dispositivos externos conectados em máquinas Windows (wireless, impressoras, adaptadores de rede, modems, dispositivos de imagem, drives de disco externo, DVD/CDROM, bluetooth);

3.190. Inventário de aplicações instaladas em ambientes Windows e Mac;

3.191. Inventário de switches com informação de número de dispositivos conectados por porta.

3.192. Deve permitir integrar-se com bases de dados e soluções externas para atualização imediata de informações de inventário de dispositivos existentes e de novos dispositivos que se conectarem à rede usando SQL e Web Services;

3.193. Deve permitir a criação de listas baseadas no inventário, tais como listas de aplicações autorizadas e nãoautorizadas.

3.194. CONSOLE DE GERENCIAMENTO
3.195. Toda informação detectada deverá ser unificada em uma única console de gerenciamento central oferecida pelo próprio fabricante capaz de gerenciar múltiplos appliances;

3.196. A Console de Gerenciamento Central deve ser capaz de atribuir a cada appliance o conjunto de segmentos de rede a ser monitorado/controlado por cada um;

3.197. Deverá possuir painéis/telas que apresentem:

3.198. Políticas, regras e detalhes dos dispositivos que caíram no escopo e nas regras estabelecidas com capacidade de filtragem por segmento, unidade organizacional e grupos e mecanismo de busca baseado em texto;

3.199. A tela/painel deverá mostrar tabela customizável com detalhes dos dispositivos, como:

3.200. Endereço Mac; 3.201. Endereço IP;

3.202. Segmento de rede;

3.203. Nome DNS e NetBIOS; 3.204. Switch, porta e VLAN de conexão do dispositivo;

3.205. Nome/Login do usuário;

3.206. Ações executadas sobre o dispositivo. 3.207. Deve ser possível customizar as propriedades dos dispositivos a serem apresentados na tabela; 3.208. Para cada máquina selecionada na tela/painel deverá ser possível:

3.209. Visualizar as políticas e regras em que o dispositivo foi enquadrado, informando data e hora, e as políticas e regras em que o dispositivo não foi enquadrado informando a razão de o mesmo não ter sido avaliado;

3.210. Exibir todos os detalhes (atributos e propriedades) do dispositivo selecionado;

3.211. Informações de compliance do dispositivo selecionado:

3.212. Inventário de usuários, dispositivos, aplicações e informações de rede com capacidade de filtragem por segmento, unidade organizacional e grupos e mecanismo de busca baseado em texto;

3.213. Criação, modificação e configuração de políticas;

3.214. Ameaças detectadas com capacidade de filtragem por segmento, unidade organizacional e grupos e mecanismo de busca baseado em texto.

3.215. Deve possuir assistente web de customização de aparência das telas de notificação e login via HTTP e do portal de gerenciamento de convidados;

3.216. Deve permitir que aplicações de terceiros consultem e atualizem propriedades/atributos dos dispositivos através de chamadas de Web Services disponíveis na solução.

3.217. Deve possuir portal WEB para consulta rápida de todos os detalhes dos dispositivos com facilidade de busca baseada em atributos do dispositivo, no mínimo por endereço IPv4, endereço IPv6, login do usuário, nome DNS, IP do switch onde o dispositivo está conectado, NetBios Domain, NetBios Hostname, e VMWare ESXi Server Name;

3.218. Deve permitir a visualização de registro de auditoria, contendo informações sobre as atividades dos administradores da solução em um período de tempo específico;

3.219. Deve permitir a visualização de log de eventos detectados pelas políticas da solução, atualizado em tempo real e filtrado por faixa de endereços IP e período de tempo, para permitir a investigação das atividades de dispositivos específicos;

3.220. Deve permitir a visualização dos logs de sistema (system logs) e envio dos mesmos para um servidor Syslog externo;

3.221. Deve fornecer opção de remediação, restrição de acesso e comunicação com o usuário final diretamente a partir da console, no mínimo:

3.222. Criar exceções para dispositivo;

3.223. Reverificar status do dispositivo;

3.224. Bloquear ou colocar em quarentena máquina em uma VLAN;

3.225. Bloquear acesso à internet;

3.226. Finalizar um processo;

3.227. Forçar autenticação na rede;

3.228. Possibilitar realizar a reverificação do dispositivo, por demanda, para todas as políticas ou apenas as selecionadas;

3.229. Possibilitar filtrar dispositivos baseado em segmentos de rede, unidades organizacionais e grupos;

3.230. Possibilitar visualizar apenas os dispositivos submetidos à classificação passiva;

3.231. Deve possuir mecanismos de limitação (threshold) de aplicação de ações de bloqueio e limitação de acesso baseado em percentual do número de dispositivos controlados, incluindo, pelo menos, as ações de desabilitar porta de switch, modificação de VLAN, TCP Reset (Firewall Virtual), notificação via HTTP, redirecionamento via HTTP e matar processos em máquinas Windows.

3.232. RELATÓRIOS E DASHBOARD

3.233. Deve possuir facilidade para geração e agendamento de relatórios com informações de tempo real sobre políticas, compliance de dispositivos, vulnerabilidades de máquinas Windows, informações do inventário, detalhes de dispositivos, ativos de rede e usuários visitantes; 4.

3.234. Deve possuir relatório/gráfico de tendência de políticas ao longo do tempo para permitir a avaliação da evolução de questões de classificação e compliance de dispositivos;

3.235. Todos os relatórios devem poder ser filtrados, pelo menos, por segmento de rede;

3.236. Todos os relatórios devem permitir agendamento e envio por e-mail;

3.237. Os relatórios que apresentem detalhes dos dispositivos devem permitir ao administrador selecionar, dentre todos os atributos dos dispositivos, aqueles que devem ser apresentados no relatório;

3.238. Deve possuir dashboard customizável que apresente de forma gráfica e dinâmica informações de classificação, conformidade e estado de gerenciamento dos dispositivos;

3.239. O dashboard deve ser composto por Widgets customizáveis que apresentem gráficos com dados estatísticos coletados das políticas e regras de classificação/compliance criadas pelo administrador;
3.240. Os Widgets devem permitir modificar dinamicamente o período de tempo apresentado no gráfico;

3.241. Os Widgets que apresentem gráficos de tendência de regras de compliance devem possuir setas indicativas de tendências de melhoria ou piora nos seus níveis:

3.242. Deve ser possível customizar o sentido das setas indicativas para indicar qual das direções (cima/baixo) indica melhoria do nível de compliance;

4. SERVIÇOS GERENCIADOS COM MONITORAMENTO E RESPOSTA A OCORRÊNCIAS APLICÁVEL AOS ITENS 1, 2, 3 e 4

4.1. Características do Serviço

4.2. A **CONTRATADA** será responsável por projetar, instalar, configurar, gerenciar e monitorar a solução ofertada;

4.3. A **CONTRATADA** deverá elaborar um projeto de implantação contendo gerenciamento de escopo, risco, mudanças, cronograma de instalação, gerenciamento de recursos humanos, contendo planejamento detalhado para permitir uma instalação com o menor risco de impacto possível, detalhando o passo a passo dos serviços;

4.4. A **CONTRATADA** deverá cumprir com todas as exigências técnicas e funcionais relacionadas com a solução ofertada, que devem ser implantadas durante o período contratado, sem ônus para o **CONTRATANTE**;

4.5. O fornecimento de toda e qualquer ferramenta, instrumento, material e equipamento de proteção, bem como materiais complementares estritamente necessários à instalação ou à assistência técnica é de inteira responsabilidade da **CONTRATADA** e não deverá gerar ônus ao **CONTRATANTE**;

4.6. No processo de instalação o Responsável Técnico deverá tomar todas as medidas necessárias visando garantir a perfeita execução do serviço (instalação e configuração);

4.7. No prazo de até 10 (dez) dias após a conclusão de instalação da solução ofertada, a contratada deverá fornecer documentação final contendo as configurações e topologias de como foi instalada a solução;

4.8. A documentação deverá ser aprovada pelo **CONTRATANTE** e pelo Gestor Técnico do **CONTRATANTE**, caracterizando a homologação da solução em um prazo de 5 dias, quando o **CONTRATANTE** emitirá um Termo de Aceite Definitivo (TAD);

4.9. Caso seja identificado defeito ou falha sistemática em determinado produto/serviço entregue pela **CONTRATADA**, ou ainda, que nos testes realizados sejam considerados em desacordo com as especificações técnicas requeridas, a o Gestor Técnico do **CONTRATANTE** pode exigir a substituição, total ou parcial, do referido produto;

4.10. A **CONTRATADA** será responsável pelo monitoramento da solução em regime 24x7, devendo manter a mesma sempre atualizada e em operação;

4.11. O monitoramento deverá ser realizado através de ferramentas próprias da **CONTRATADA** integradas via API com a console/servidor de gerenciamento central para automação de coleta de alertas críticos e acionamento imediato da equipe da **CONTRATADA**;

4.12. A ocorrência de alertas de alta criticidade devem acionar diretamente, de forma automática, através de alarme sonoro em aplicativo de celular, os técnicos de plantão da **CONTRATADA** para início imediato do tratamento da ocorrência, dentro dos prazos definidos no ANS, sendo reportados imediatamente ao preposto do **CONTRATANTE** para ciência do fato;
4.13. A **CONTRATADA** deverá informar mensalmente a escala de técnicos de sobreaviso que atenderão os alertas de alta criticidade durante o período do plantão;
4.14. À opção do **CONTRATANTE**, esta poderá indicar até 5 profissionais para receberem os alarmes em tempo real, de forma simultânea, no aplicativo de celular a ser fornecido pela **CONTRATADA** sem custos adicionais.

4.15. O tratamento das ocorrências geradas pelo sistema de monitoramento automático deve ser acompanhado através de plataforma de gestão automatizada de processos (BPMn) fornecido pela **CONTRATADA**, que indique claramente e controle os prazos para execução de cada etapa do processo de resposta aos incidentes detectados;

4.16. O processo de tratamento de incidentes deve conter pelo menos as seguintes características:

4.17. Notificação imediata da **CONTRATADA** sobre a ocorrência detectada;

4.18. Investigação da ocorrência através dos recursos fornecidos pela solução;

4.19. Determinação da real criticidade da ocorrência;

4.20. Execução de ações de contenção previamente acordadas com o cliente;

4.21. O processo automatizado deve ser capaz de tratar de forma diferenciada pelo menos 4 níveis de criticidade de alertas;

4.22. O processo automatizado deve ser capaz de enviar e-mail e alertas em aplicativo de celular de forma automática para a **CONTRATADA** e para o **CONTRATANTE**;

4.23. O processo automatizado deve ser capaz de emitir avisos sonoros através de aplicativo de celular para os técnicos da **CONTRATADA** e do **CONTRATANTE**, com diferentes graus de intensidade a depender do nível de criticidade da situação detectada;

4.24. Deve permitir a customização, para cada **CONTRATANTE**, de quais tipos de alertas se enquadram em cada um dos níveis de criticidade.

4.25. Deve ser disponibilizado para o **CONTRATANTE** um dashboard de acompanhamento em tempo real dos processos de tratamento dos incidentes que apresente, no mínimo:

4.25.1. Tarefas em aberto com indicação do responsável pela sua execução e tempo restante para finalização da mesma de acordo com o ANS contratado;

4.25.2. Tarefas em atraso com indicação do responsável pela sua execução e tempo de atraso em relação ao ANS contratado;

4.25.3. Tabela de atraso médio de tarefas já encerradas;

4.25.4. Tabela de tempo médio de execução de tarefas já encerradas.

4.26. A manutenção visa manter em perfeito estado de operação os serviços fornecidos em atendimento ao objeto, deste modo a **CONTRATADA** deve cumprir os seguintes procedimentos:

4.26.1. desinstalação, reconfiguração ou reinstalação decorrentes de falhas no software, atualização da versão de software, correção de defeitos, ajustes e reparos necessários, de acordo com os manuais e as normas técnicas específicas para os recursos utilizados;

4.26.2. Quanto às atualizações pertinentes aos softwares, entende-se como "atualização" o provimento de toda e qualquer evolução de software, incluindo correções, "patches", "fixes", "updates", "service packs", novas "releases", "versions", "builds", "upgrades", englobando inclusive versões não sucessivas, nos casos em que a liberação de tais versões ocorra durante o período de garantia especificado.
4.27. Deve ser elaborado e enviado mensalmente um relatório executivo com o resumo das principais ocorrências e as providências executadas pela **CONTRATADA**, além de gráficos e estatísticas relativos à conformidade operacional do ambiente;

4.28. A operação e administração (gerenciamento total) da solução será realizada pela **CONTRATADA** conforme as orientações e solicitações de configurações e políticas realizadas pelo Gestor Técnico do **CONTRATANTE**;

4.29. As solicitações de alteração de configurações deverão ser realizadas conforme o ANS definido na Seção – Acordo de Nível de Serviço – ANS;

4.30. No caso de necessidade de ações preventivas ou corretivas o **CONTRATANTE** agendará com antecedência junto a **CONTRATADA** as implementações das correções, fora do horário comercial, preferencialmente em feriados e finais de semana. Nenhuma ação poderá ser executada sem a ciência e anuência do **CONTRATANTE**;

4.31. A **CONTRATADA** deverá prestar suporte a todos os componentes de software fornecidos para a implementação e utilização da solução;

4.32. A **CONTRATADA** deverá disponibilizar serviço de suporte técnico e manutenção, no regime (24x7) vinte e quatro horas por dia, sete dias por semana, pelo período da contratação;

4.33. Os acionamentos dos serviços de suporte e manutenção serão requisitados por meio de ordens de serviço, a serem abertas pelo **CONTRATANTE**, através de número de telefone nacional (0800 com serviço de uso ilimitado) disponibilizado pela **CONTRATADA**, e ainda, por e-mail e sítio de internet;

4.34. Não haverá limitação no número de chamados que poderão ser abertos;

4.35. A **CONTRATADA** manterá registro de todas as ordens de serviço abertas, disponibilizando, para cada uma, no mínimo as seguintes informações:

4.35.1. Número sequencial da ordem;

4.35.2. Data e hora de abertura;

4.35.3. Severidade;

4.35.4. Descrição do problema;

4.35.5. Data e hora do início do atendimento;

4.35.6. Data e hora de término do atendimento (solução).

4.36. O serviço de suporte técnico e manutenção deverá ser prestado por profissional devidamente certificado nas soluções tecnológicas utilizadas na prestação dos serviços contratados;

4.37. As informações relacionadas à ANS estão na Seção – Acordo de Nível de Serviço – ANS.

4.38. Acordo de Nível de Serviço (ANS)

4.39. A **CONTRATADA** deverá possuir Central de Atendimento (contato telefônico, sítio na Internet e e-mail) para consultas, aberturas de chamados técnicos e envio de arquivos para análise, durante 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana;

4.40. A **CONTRATADA** deverá prestar serviços de suporte técnico 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, na cidade de Salvador – BA, relativos ao objeto deste Termo de Referência, sem ônus para o **CONTRATANTE**;
4.41. A **CONTRATADA** será responsável pelo cumprimento e medição dos índices estabelecidos neste item que serão auditados pelo **CONTRATANTE** durante todo o prazo de vigência do contrato, e que poderão ser revistos, a qualquer tempo, com vistas à melhoria ou ajustes na qualidade dos serviços prestados, mediante acordo entre as partes;

4.42. Níveis de Serviço e Tempo Esperados:

4.43. Plantão Telefônico por número 0800 como serviço de uso ilimitado, no período de 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana;

4.44. No Local (on site) – Serviço de uso ilimitado, prestado em caso de emergência, ou outra necessidade maior e também compreendendo os seguintes tipos de atendimento local: suporte para upgrade de versões e releases do software; solução de problemas detectados (troubleshoot); análise e correção de eventos relacionados à segurança e à performance do software e do ambiente; atualização simultânea nos ambientes dos Órgãos e Entidades do **CONTRATANTE**.

4.45. Para efeito dos atendimentos técnicos, a **CONTRATADA** deverá observar os níveis de severidade e respectivos prazos máximos fixados abaixo:

4.46. NÍVEIS DE SEVERIDADE DOS CHAMADOS

NÍVEIS DE SEVERIDADE DOS CHAMADOS	
NÍVEL	**DESCRIÇÃO**
1	Serviços totalmente indisponíveis
2	Serviços parcialmente indisponíveis ou com degradação de tempo de resposta no acesso aos aplicativos
3	Serviços disponíveis com ocorrência de alarmes de avisos, consultas sobre problemas, dúvidas gerais sobre o equipamento fornecido

TABELA DE PRAZOS DE ATENDIMENTO AO SOFTWARE				
MODALIDADE	**PRAZOS**	**1**	**2**	**3**
	Início atendimento	2 horas	4 horas	24 horas

On site	Término atendimento	4 horas	8 horas	72 horas
Telefone, email e web	Início atendimento	2 horas	4 horas	24 horas
	Término atendimento	4 horas	8 horas	72 horas

4.47. Para o Nível 1, caso o atendimento não seja finalizado até as 20h00min, o técnico não poderá interrompêlo, devendo continuar até sua finalização, ou a interrupção do mesmo pelo **CONTRATANTE** através do Gestor do Contrato;

4.48. Após a conclusão do serviço é obrigação da **CONTRATADA** verificar o restabelecimento das condições operacionais normais;

4.49. Todo chamado somente será caracterizado como "encerrado" mediante concordância do **CONTRATANTE**;

4.50. Todo chamado de incidente, após sua solução, deverá ser finalizado com a emissão de um Relatório de Incidente a ser enviado para o **CONTRATANTE**.

4.51. Para as situações em que a solução definitiva de problemas no ambiente demande reimplantação, reestruturação ou reinstalação do produto, este deverá ser programado e planejado, com a antecedência necessária, de modo a não prejudicar a operação dos demais sistemas do **CONTRATANTE**.

APENSO II

TERMO DE COMPROMISSO DE SIGILO

O **MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA**, sediado em 5ª Avenida, n° 750, CAB - Salvador, BA - Brasil - CEP: 41.745-004, CNPJ n.º 04.142.491/0001-66, doravante denominado **CONTRATANTE**, e, de outro lado, a **CENTRO DE PESQUISAS EM INFORMÁTICA LTDA**, sediada à Av. Santos Dumont, 6216, S331 Quadra única, Loteamento Jardim Santo Antônio, Pitangueiras, Lauro de Freitas/BA, CEP 42.701-260, CNPJ n.º 40.584.096/0002-88 doravante denominada CONTRATADA;

CONSIDERANDO que, em razão do CONTRATO N.º 095/2025, a **CONTRATADA** poderá ter acesso a informações sigilosas do **CONTRATANTE**;

CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção;

CONSIDERANDO o disposto na Política de Segurança da Informação do Contratante;

Resolvem celebrar o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO, doravante TERMO, vinculado ao CONTRATO N.º 095/2025, mediante as seguintes cláusulas e condições:

Cláusula Primeira – DO OBJETO

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela Contratada, no que diz respeito ao trato de informações sigilosas, disponibilizadas pelo **CONTRATANTE**, por força dos procedimentos necessários para a execução do objeto do contrato celebrado entre as partes e em acordo com o que dispõem a Lei nº 12.527, de 18/11/2011 e os Decretos nº 7.724, de 16/05/2012 e 7.845, de 14/11/2012, que regulamentam os procedimentos para acesso e tratamento de informação classificada em qualquer grau de sigilo.

Cláusula Segunda – DOS CONCEITOS E DEFINIÇÕES

Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:

INFORMAÇÃO: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

INFORMAÇÃO SIGILOSA: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado.

Cláusula Terceira – DA INFORMAÇÃO SIGILOSA

Serão consideradas como informação sigilosa, toda e qualquer informação classificada ou não nos graus de sigilo ultrassecreto, secreto e reservado. O TERMO abrangerá toda informação escrita, verbal ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: know-how, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as atividades do **CONTRATANTE** e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não do contrato celebrado entre as partes, doravante denominados INFORMAÇÕES, a que diretamente ou pelos seus empregados, a **CONTRATADA** venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO nº 095/2025.

Cláusula Quarta – DOS LIMITES DO SIGILO

As obrigações constantes deste TERMO não serão aplicadas às INFORMAÇÕES que:

I – Sejam comprovadamente de domínio público no momento da revelação, exceto se tal fato decorrer de ato ou omissão da **CONTRATADA**;

II – Tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente TERMO;

III – Sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

Cláusula Quinta – DOS DIREITOS E OBRIGAÇÕES

As partes se comprometem a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do contrato celebrado entre as partes, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas INFORMAÇÕES, que se restringem estritamente ao cumprimento do contrato ao qual se vincula o presente termo.

Parágrafo Primeiro – A **CONTRATADA** se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento expresso e prévio do **CONTRATANTE**.

Parágrafo Segundo – A **CONTRATADA** compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do

contrato ao qual se vincula o presente instrumento sobre a existência deste TERMO bem como da natureza sigilosa das informações.

I – A **CONTRATADA** deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente TERMO e dará ciência ao **CONTRATANTE** dos documentos comprobatórios.

Parágrafo Terceiro – A **CONTRATADA** obriga-se a tomar todas as medidas necessárias à proteção da informação sigilosa do **CONTRATANTE**, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pelo **CONTRATANTE**.

Parágrafo Quarto – Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste TERMO.

I – Quando requeridas, as INFORMAÇÕES deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes.

Parágrafo Quinto - A **CONTRATADA** obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados e contratados, assim como por quaisquer outras pessoas vinculadas à Contratada, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do contrato celebrado entre as partes a qual se vincula o presente termo.

Parágrafo Sexto - A **CONTRATADA**, na forma disposta no parágrafo primeiro, acima, também se obriga a:

I. Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das INFORMAÇÕES, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;
II. Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmo judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das INFORMAÇÕES por seus agentes, representantes ou por terceiros;

III. Comunicar ao **CONTRATANTE**, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das INFORMAÇÕES, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e

IV. Identificar as pessoas que, em nome da **CONTRATADA**, terão acesso às informações sigilosas.

Cláusula Sexta – DA VIGÊNCIA

O presente TERMO tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de sua assinatura até expirar o prazo de classificação da informação a que a **CONTRATADA** teve acesso em razão do contrato ao qual se vincula o presente instrumento.

A vigência deste Termo independe do prazo de vigência do contrato assinado.

Cláusula Sétima – DAS PENALIDADES

A quebra do sigilo e/ou da confidencialidade das INFORMAÇÕES, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do contrato ao qual se vincula o presente instrumento. Neste caso, A **CONTRATADA**, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pelo Contratante, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis.

Cláusula Oitava – DISPOSIÇÕES GERAIS

Este TERMO de Confidencialidade é parte integrante e inseparável do CONTRATO nº 095/2025.

Parágrafo Primeiro – Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa-fé, da equidade, da razoabilidade, da economicidade e da moralidade.

Parágrafo Segundo – O disposto no presente TERMO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tal como aqui definidas.

Parágrafo Terceiro - Havendo necessidade legal devido a Programas de Governo, A **CONTRATADA** assume o compromisso de assinar Termo de Sigilo (ou equivalente) adicional relacionado ao Programa, prevalecendo as cláusulas mais restritivas em benefício do **CONTRATANTE**.

Parágrafo Quarto – Ao assinar o presente instrumento, A **CONTRATADA** manifesta sua concordância no sentido de que:

I. O **CONTRATANTE** terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da Contratada;
II. A **CONTRATADA** deverá disponibilizar, sempre que solicitadas formalmente pelo Contratante, todas as informações requeri das pertinentes ao contrato ao qual se vincula o presente termo;

III. A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo;

IV. Todas as condições, TERMOS e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes;

V. O presente TERMO somente poderá ser alterado mediante TERMO aditivo firmado pelas partes;

VI. Alterações do número, natureza e quantidade das informações disponibilizadas para a **CONTRATADA** não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

VII. O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações disponibilizadas para a **CONTRATADA**, serão incorporados a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas;

VIII. Este TERMO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar INFORMAÇÕES para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

Cláusula Nona – DO FORO

Fica eleito o foro da comarca de Salvador, onde está localizada a sede do **CONTRATANTE**, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO é assinado pelas partes para que produza seus regulares efeitos.

_____, _____ de _____ de 20____

De acordo.

CONTRATANTE

MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA
André Luis Sant´Ana Ribeiro
Superintendente de Gestão Administrativa

CONTRATADA

CENTRO DE PESQUISAS EM INFORMÁTICA LTDA
João Gualberto Rizzo Araújo
sócio – administrador

CONTRATO DE PRESTAÇÃO DE SERVIÇOS –
PROCEDIMENTO SEI 19.09.02684.0009580/2025-72.

CONTRATO DE PRESTAÇÃO DE SERVIÇOS QUE ENTRE SI CELEBRAM O MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA E O CENTRO DE PESQUISAS EM INFORMATICA LTDA, NA FORMA ABAIXO:

CONTRATO Nº 095/2025 - 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 **André Luis Sant´Ana Ribeiro**, doravante denominado **CONTRATANTE**, e o **Centro de Pesquisas em Informática Ltda**, CNPJ nº. 40.584.096/0002-88, estabelecida à Av. Santos Dumont, 6216, S331 Quadra única, Loteamento Jardim Santo Antônio, Pitangueiras, Lauro de Freitas/BA, CEP 42.701-260, representada por seu sócio - administrador Sr. **João Gualberto Rizzo Araújo,** inscrito no CPF/MF sob o nº 50*******20, doravante denominada **CONTRATADA**, com supedâneo no quanto disposto na Lei Federal nº 14.133/2021 e na Lei Estadual/Ba nº 14.634/2023, e, ainda, observado o constante no Processo de Licitação, **Pregão Eletrônico nº 90015/2025**, protocolado sob o nº 19.09.02684.0009580/2025-72, o qual integra este instrumento independentemente de transcrição, **CELEBRAM** o presente Contrato, mediante as cláusulas e condições seguintes:

CLÁUSULA PRIMEIRA - DO OBJETO

1.1 O presente instrumento tem por objeto contratação de empresa para prestação de serviços Gerenciados de Soluções de Segurança para proteção dos dispositivos, estações de trabalho e servidores, incluindo capacidade estendida de prevenção, detecção e resposta, acesso remoto seguro, gestão de vulnerabilidades, visibilidade, garantias de conformidade, controle de acesso e automação, não apenas para os dispositivos, mas também para os usuários, bem como serviços de instalação, treinamento, gerenciamento, manutenção e atualização das soluções, garantias de conformidade e resposta a incidentes para a equipe do Ministério Público do Estado da Bahia, em regime 24x7, com atendimento on-site, conforme condições estabelecidas neste instrumento;

1.2 A **CONTRATADA** se declara em condições de prestar o serviço objeto deste instrumento em estrita observância com o disposto neste contrato.

1.3 A assinatura do presente instrumento contratual, pela **CONTRATADA**, importa na presunção de plena ciência e aquiescência com o seu conteúdo, inclusive quanto aos documentos anexos.

CLÁUSULA SEGUNDA – DA VINCULAÇÃO AO EDITAL DO CERTAME LICITATÓRIO

Integram o presente contrato, vinculando esta contratação, independentemente de transcrição: o termo de referência, a proposta da contratada e eventuais anexos dos documentos supracitados, além das condições estabelecidas no edital do certame, que o originou, referido no preâmbulo deste instrumento.

CLÁUSULA TERCEIRA – DA DURAÇÃO DO CONTRATO

3.1 O prazo de vigência do presente Contrato é de 36 (trinta e seis) meses, a contar da data da (última) assinatura pelas partes, admitindo-se a sua prorrogação por sucessivos períodos, limitados a 10 (dez) anos, nos termos dos artigos 106 e 107 c/c artigo 6º, XV da Lei Federal nº 14.133/2021, e será formalizada por termo aditivo;

3.1.1 A prorrogação de que trata este dispositivo é condicionada ao ateste, pela autoridade competente, de que as condições e os preços permanecem vantajosos para a Administração, permitida a negociação com a **CONTRATADA**;

3.1.2 A prorrogação do prazo de vigência contratual fica condicionada, ademais, à disponibilidade orçamentária, devidamente declarada pela Unidade Gestora do recurso nos autos do procedimento administrativo correspondente.

CLÁUSULA QUARTA - DO REGIME, DA FORMA DE EXECUÇÃO E DOS PRAZOS PARA EXECUÇÃO

4.1 O Regime de execução do presente Contrato é de Execução Indireta na modalidade Empreitada por Preço Global;

4.2 O **CONTRATANTE** convocará a **CONTRATADA** para retirar a nota de empenho no prazo de até 05 (cinco) dias corridos contado a partir da notificação pela Administração, que ocorrerá, preferencialmente, através de envio de e-mail para o endereço indicado na proposta de preços;

4.2.1 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).

4.2.2 A Contratada poderá solicitar a prorrogação do prazo para retirada/recebimento da nota de empenho, por motivo justo e aceito pela Administração.

4.3 Os serviços deverão ser executados no seguinte endereço: Sede Administrativa: 5ª Avenida, n° 750, do CAB - Salvador no horário das 8:00h às 12h e das 14h às 18h endereço, em dias expediente administrativo – segunda a sexta;

4.4 Para realização dos serviços é necessário o prévio agendamento juntamente com a Diretoria de Tecnologia da Informação – Coordenação de Assessoramento em Segurança da Informação, através dos contatos (071 3103-0214 e iassa@mpba.mp.br. A Diretoria de Tecnologia da Informação – Coordenação de Assessoramento em Segurança da Informação é o responsável por acompanhar a execução;

4.5 O prazo de início de execução do objeto é de até 30 (trinta) dias úteis contados do dia útil subsequente ao recebimento da Nota de Empenho, Contrato ou documento equivalente;

4.6 Os serviços serão prestados nas seguintes condições:

Serviços/Etapas	**Condições**	**Cronograma de Execução**
01	Entrega do licenciamento	5 dias
02	Kick off, preparação das máquinas virtuais, planejamento/execução de possíveis implantação das soluções migrações,	20 dias
03	Treinamento	5 dias

4.7 Devidamente justificado e com pelo menos 15 dias corridos de antecedência do prazo final de execução, o prestador de serviço poderá solicitar prorrogação de prazo, ficando a cargo da área demandante acolher a solicitação, desde que não haja prejuízo, ressalvadas situações de caso fortuito e força maior;

4.8 Para a perfeita execução dos serviços, o prestador do serviço deverá disponibilizar os materiais, equipamentos, ferramentas e utensílios necessários, nas quantidades estimadas e qualidades a seguir estabelecidas, promovendo sua substituição quando necessário;

4.9 O prestador de serviço se obriga a executar o objeto em conformidade com as especificações descritas na Proposta de Preços e neste Termo de Referência, sendo de sua inteira responsabilidade a substituição, caso não esteja em conformidade com as referidas especificações;

4.10 Todas as despesas relativas à execução do objeto licitado, bem como todos os impostos, taxas e demais despesas decorrentes do futuro contrato correrão por conta exclusiva do prestador de serviço;

4.11 Demais especificações técnicas relativas à solução encontram-se detalhadas nas especificações técnicas detalhadas.

CLÁUSULA QUINTA – DO RECEBIMENTO DO OBJETO

5.1 O recebimento provisório dos serviços será realizado mediante termo detalhado emitido pelo fiscal técnico, relativamente ao cumprimento dos prazos de execução e demais exigências de caráter técnico, devendo ocorrer em até 05 (cinco) dias corridos;

5.1.1 O prazo de que trata o subitem anterior será contado do recebimento de comunicação escrita do fornecedor com a comprovação da prestação dos serviços a que se refere a parcela a ser paga;

5.2 Os serviços poderão ser rejeitados, no todo ou em parte, inclusive antes do recebimento provisório, quando em desacordo com as especificações constantes neste Termo de Referência e na Proposta de preços, devendo ser refeitos no prazo de 05 (cinco) dias corridos, a contar da intimação do fornecedor, às suas custas, sem prejuízo da aplicação das penalidades, cabendo à fiscalização não atestar o recebimento até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório;

5.3 Quando a fiscalização for exercida por um único servidor, o termo detalhado de recebimento provisório deverá conter o registro, a análise e a conclusão sobre todas as ocorrências na execução do Contrato, acompanhado dos demais documentos que julgar necessários, encaminhando-o ao servidor ou comissão designada pela autoridade competente para recebimento definitivo.

5.4 Os serviços serão recebidos definitivamente, em até 20 (vinte dias) dias corridos], contados do recebimento provisório, pelo gestor do contrato ou comissão designada pelo Superintendente de Gestão Administrativa, mediante termo detalhado que comprove o atendimento de todas as exigências contratuais.

5.5 O prazo para recebimento definitivo poderá ser excepcionalmente prorrogado, de forma justificada, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais.

5.6 Caso necessário, o gestor do contrato notificará o fornecedor, para realização das substituições e/ou adequações cabíveis, conforme prazo indicado no **item 5.2**;

5.7 Para efeito de recebimento provisório, ao final de cada período de faturamento, o(s) fiscal(is) do contrato deverá(ão) apurar o resultado das avaliações da execução do objeto e, se for o caso, a análise do desempenho e qualidade da prestação dos serviços realizados em consonância com os indicadores previstos;

5.7.1 A análise do desempenho e qualidade da prestação dos serviços referida no subitem anterior poderá resultar no redimensionamento de valores a serem pagos ao fornecedor, circunstância que deverá ser registrada pelo(s) fiscal(is) em relatório(s) a ser encaminhado ao gestor do Contrato;

5.8 A fiscalização não efetuará o ateste da última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas durante o recebimento provisório;

5.9 O MPBA rejeitará, no todo ou em parte, inclusive antes do recebimento provisório, o objeto contratual em desacordo com as condições pactuadas, podendo, entretanto, se lhe convier, decidir pelo recebimento, neste caso com as deduções cabíveis;

5.10 Em caso de recusa, no todo ou em parte, do objeto contratado, fica o fornecedor obrigado a substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, conforme prazo indicado no **item 5.2**, cabendo ao Gestor do Contrato somente habilitar para pagamento a(s) parcela(s) recebida(s) em conformidade;

5.11 O recebimento definitivo do objeto deste instrumento será concretizado depois de adotados, pelo MPBA, todos os procedimentos cabíveis em Ato Normativo próprio, no art. 140 da Lei Federal nº 14.133/2021 e, no que couber, da Lei Estadual de nº 14.634/2023, devendo ocorrer no prazo indicado no **item 5.4;**

5.12 Nenhum prazo de recebimento ocorrerá enquanto pendente a solução, pela contratada, de inconsistências verificadas na execução do objeto ou nota(s) fiscal(is) ou

instrumento(s) de cobrança equivalente(s);

5.13 O aceite ou aprovação do objeto pelo MPBA não exclui a responsabilidade do fornecedor pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do Contrato; **CLÁUSULA SEXTA – DO PREÇO**

6.1 O preço unitário estabelecido para a plena execução do objeto contratual se encontra descrito na tabela abaixo:

ITEM	DESCRIÇÃO DO SERVIÇO	UNIDADE DE MEDIDA	QUANTIDADE	PREÇO UNITÁRIO	PREÇO TOTAL
1	Serviços gerenciados de soluções de segurança para plataforma SSE com controle de acesso remoto, pelo período de 36 meses	Unidade	500	R$ 1.535,46	R$ 767.730,00
2	Serviços gerenciados de Gestão de exposição cibernética por 36 meses	Unidade	4500	R$ 1.017,26	R$ 4.577.670,00
3	Serviços gerenciados de visibilidade, conformidade, segurança e orquestração dos dispositivos conectados à rede corporativa por 36 meses	Unidade	4000	R$ 409,00	R$ 1.636.000,00
VALOR GLOBAL					R$ 6.981.400,00

6.2 Dá-se ao presente Contrato o valor global de **R$ 6.981.400,00 (seis milhões novecentos e oitenta e um mil e quatrocentos reais)**, equivalente ao período total de vigência da contratação;

6.3 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 da **CONTRATADA** envolvido na execução do objeto, materiais empregados, inclusive ferramentas e fardamentos, combustíveis, lubrificantes, manutenção, lavagens, estacionamento, depreciação, aluguéis, seguros, franquias, administração, tributos e emolumentos.

CLÁUSULA SÉTIMA - DO PAGAMENTO E DA ATUALIZAÇÃO MONETÁRIA

7.1 Os pagamentos serão processados conforme ordem cronológica de pagamento, nos termos disciplinados no art.141 da Lei Federal de nº14.133/21;

7.2 O faturamento referente ao objeto deste contrato será efetuado em 03 (três) parcelas anuais de igual valor, correspondentes ao percentual de 33,33% do serviço total;

7.3 O pagamento será processado mediante apresentação, pela **CONTRATADA**, de fatura, Nota Fiscal relativa à prestação dos serviços e certidões de regularidade cabíveis, bem como consulta à situação de idoneidade da
CONTRATADA, documentação que deverá estar devidamente acompanhada do **TERMO DE RECEBIMENTO** pelo **CONTRATANTE**;

7.4 Os pagamentos serão processados no prazo de 20 (vinte) dias úteis, a contar da data de apresentação da documentação indicada no **item 7.3**, desde que não haja pendência a ser regularizada;

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

7.4.2 No caso de controvérsia sobre a execução do objeto, quanto a dimensão, qualidade e quantidade, a parcela incontroversa deverá ser liberada no prazo previsto para pagamento;

7.5 As faturas far-se-ão acompanhar da documentação probatória relativa ao recolhimento dos tributos que tenham como fato gerador o objeto consignado na **Cláusula Primeira**;

7.6 O **CONTRATANTE** realizará a retenção de impostos ou outras obrigações de natureza tributária, de acordo com a legislação vigente;

7.7 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;

7.8 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 nos **itens 7.4 e 7.4.1.**

7.8.1 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**.

7.9 No ato de liquidação da despesa, os serviços de contabilidade comunicarão aos órgãos da administração tributária as características da despesa e os valores pagos, conforme o disposto no art. 63 da Lei nº 4.320, de 17 de março de 1964.

CLÁUSULA OITAVA – DA MANUTENÇÃO DO EQUILÍBRIO ECONÔMICO-FINANCEIRO DO CONTRATO

8.1 A concessão de reajustamento ocorrerá após o transcurso do prazo de 01 (um) ano da data do orçamento estimado pela Administração, qual seja, 09 de abril de 2025, mediante aplicação do IPCA relativo ao período decorrido entre a referida data e a data da efetiva concessão do reajuste;

8.1.1 Nos reajustes subsequentes ao primeiro, o interregno mínimo de 01 (um) ano será contado a partir dos efeitos financeiros do último reajuste;

8.1.2 Os valores reajustados incidirão sobre as parcelas de serviços a serem executadas após o prazo de que cuida o item 8.1;

8.1.3 A variação do valor contratual para fazer face ao reajuste de preços será realizada por simples apostila, dispensando a celebração de aditamento;

8.2 O reestabelecimento do equilíbrio econômico-financeiro dependerá de requerimento da Contratada quando visar recompor o preço que se tornou insuficiente, devendo ser instruído com a documentação que comprove o desequilíbrio econômico-financeiro do contrato;

8.2.1. O requerimento de restabelecimento do equilíbrio econômico-financeiro inicial do contrato, nas hipóteses do art. 124, II, "d", ou do art. 135 da Lei Federal nº 14.133, de 2021, deverá ser formulado pelo interessado no prazo máximo de um ano do fato que o ensejou, sob pena de decadência, em consonância com o art. 211 da Lei Federal nº 10.406, de 10 de janeiro de 2002;

8.2.2. Na hipótese de contratos de fornecimento contínuos, o requerimento de restabelecimento do equilíbrio econômico-financeiro deverá ser formulado durante a vigência do contrato e antes de eventual prorrogação nos termos do art. 131, parágrafo único, da Lei n° 14.133, de 2021, sob pena de preclusão;

8.2.2.1. Fica convencionado que, nos casos de contrato de fornecimento contínuos com prazo de vigência superior a 1 (um) ano, o requerimento de restabelecimento do equilíbrio econômico-financeiro do contrato deverá observar a disposição do **subitem 8.2.1**;

8.3 O **CONTRATANTE**, no prazo máximo de 60 (sessenta) dias, prorrogável por igual período mediante justificativa, responderá a eventuais pedidos de manutenção do equilíbrio econômico-financeiro do Contrato apresentado pela Contratada (art. 92, inciso XI, c/c 123, parágrafo único da Lei n° 14.133, de 2021);

8.4 O processo de reestabelecimento do equilíbrio econômico-financeiro em favor do Contratante deverá ser instaurado quando possível a redução do preço ajustado para compatibilizá-lo ao valor de mercado ou quando houver diminuição, devidamente comprovada, dos preços dos insumos básicos utilizados no Contrato.

CLÁUSULA NONA - 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
40.101/0021	2002	9900	1.500.0.100.000000.00.00.00	33.90.40

CLÁUSULA DÉCIMA - DO MODELO DE GESTÃO E FISCALIZAÇÃO CONTRATUAL

10.1 Na forma das disposições estabelecidas na Lei Federal nº 14.133/2021 e na Lei Estadual/BA nº 14.634/2023, o **CONTRATANTE** designará servidor(es), por meio de Portaria específica para tal fim, para a gestão e 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.

10.2 Incumbe à fiscalização acompanhar e verificar a perfeita execução do contrato, em todas as suas fases, competindo-lhe, primordialmente:

10.2.1 Acompanhar o cumprimento dos prazos de execução descritos neste instrumento, e determinar as providências necessárias à correção de falhas, irregularidades e/ou defeitos, sem prejuízos das sanções contratuais legais;

10.2.2 Transmitir à **CONTRATADA** as instruções, e comunicar alterações de prazos ou roteiros, quando for o caso;

10.2.3 Promover, com a presença da **CONTRATADA**, a verificação dos serviços já efetuados;

10.2.4 Esclarecer as dúvidas da **CONTRATADA**, solicitando ao setor competente do **CONTRATANTE**, se necessário, parecer de especialistas;

10.2.5 Manter anotação em registro próprio todas as ocorrências relacionadas à execução do contrato, determinando o que for necessário para a regularização das faltas ou dos defeitos observados;

10.2.6 Informar aos seus superiores, em tempo hábil para a adoção das medidas convenientes, a situação que demandar decisão ou providência que ultrapasse sua competência (Lei Estadual de nº14.634/23; art.12, §2º e Lei nº 14.133/2021, art. 117, §2º);

10.3 A fiscalização, pelo **CONTRATANTE**, não desobriga a **CONTRATADA** de sua responsabilidade quanto à perfeita execução do objeto contratual;

10.3.1 A ausência de comunicação, por parte do **CONTRATANTE**, sobre irregularidades ou falhas, não exime a **CONTRATADA** das responsabilidades determinadas neste contrato;

10.4 O **CONTRATANTE** poderá recusar, sustar e/ou determinar o desfazimento/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 ainda que atentem contra a segurança de terceiros ou de bens;

10.4.1 Qualquer serviço considerado não aceitável, no todo ou em parte, deverá ser refeito pela **CONTRATADA**, às suas expensas;

10.4.2 A não aceitação de algum serviço, no todo ou em parte, não implicará na dilação do prazo de execução, salvo expressa concordância do **CONTRATANTE**;

10.5 Caberá ao gestor do contrato deliberar sobre a execução contratual, em especial:

10.5.1 Autorizar o início da execução do objeto contratual, deliberando sobre o momento do envio de documentos de formalização tais como documentos ou nota de empenho ordinária à contratada;

10.5.2 Coordenar as atividades realizadas pelos fiscais técnico, administrativo e setorial quanto ao cumprimento de obrigações assumidas pela contratada, elaborando, sempre que necessário, relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento à finalidade da Administrativa;

10.5.3 Receber dúvidas ou questionamentos de matérias sob sua competência, feitos pelo fornecedor e/ou pela fiscalização, manifestando-se e dando o devido encaminhamento;

10.5.4 Deliberar sobre prorrogações de prazos de entre ou execução;

10.5.5 Deliberar sobre o recebimento definitivo do objeto contratado, mediante emissão de termo detalhado, quando não for designada comissão específica para tal fim;

10.5.6 Adotar as providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso;

10.6 Para fins de fiscalização e gestão o MPBA poderá solicitar ao fornecedor, a qualquer tempo, os documentos relacionados com a execução do futuro contrato;

10.7 A gestão e a fiscalização contratual observarão, ainda, as normas e regulamentos internos do Ministério Público do Estado da Bahia que venham a ser publicados para disciplina da matéria.

CLÁUSULA DÉCIMA PRIMEIRA – DAS OBRIGAÇÕES DA CONTRATADA

11.0 Além das determinações contidas na Cláusula **QUARTA** - **do Regime e da forma de execução** deste contrato e no processo de Licitação que o originou – que aqui se consideram literalmente transcritas, bem como daquelas decorrentes de lei, a **CONTRATADA**, obriga-se a:

11.1 Cumprir todas as obrigações constantes no Edital, seus anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto;

11.2 Efetuar a execução do objeto em perfeitas condições, conforme especificações, prazo e local constantes neste Termo de Referência e seus apensos, acompanhado da respectiva nota fiscal com todas as discriminações inerentes ao objeto, bem como as certidões de regularidade cabíveis;

11.3 Responder por quaisquer danos e prejuízos causados em função do objeto do contrato a ser firmado, bem como por todos os danos e prejuízos decorrentes de paralizações na execução dos serviços, salvo na ocorrência de motivo de força maior, apurados na forma da legislação vigente, e desde que comunicados ao MPBA no prazo de 48 horas do fato, ou da ordem expressa escrita do MPBA;

11.4 Reparar, corrigir, remover, reconstruir ou substituir, total ou parcialmente, às suas expensas, no prazo fixado neste Termo de Referência, o objeto do futuro contrato em que se verifiquem má qualidade, vícios, defeitos ou incorreções, resultantes de execução irregular, do emprego de materiais ou equipamentos inadequados, se for o caso, ou não correspondente(s) ao(s) material(is);

11.5 Comunicar ao MPBA, no prazo de 48 horas que antecede a data da execução, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação;

11.6 Manter, durante toda a execução do futuro contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

11.7 Promover a destinação final ambientalmente adequada do dos materiais eventualmente empregados na prestação dos serviços, sempre que a legislação assim o exigir;
11.8 Prestar ao MPBA, sempre que necessário, esclarecimentos, fornecendo toda e qualquer orientação necessária.

11.9 Dispor de toda mão de obra, veículos, transportes, insumos, Alvarás, licenciamentos, autorizações e materiais necessários à execução do objeto deste Termo de Referência;

11.10 Assegurar que o objeto deste Termo de Referência não sofra solução de continuidade durante todo o prazo da sua vigência;

11.11 Responsabilizar-se pelo cumprimento das obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas em legislação específica na execução do objeto, cuja inadimplência não transfere a responsabilidade ao MPBA;

11.12 A eventual retenção de tributos pelo MPBA não implicará a responsabilização deste, em hipótese alguma, por quaisquer penalidades ou gravames futuros, decorrentes de inadimplemento(s) de tributos pelo fornecedor.

11.13 Emitir notas fiscais/faturas de acordo com a legislação, contendo descrição do objeto, indicação de quantidades, preços unitários e valor total, competindo ao fornecedor, ainda, observar, de acordo com a previsão da legislação tributária aplicável, nas hipóteses de retenção de tributos pelo MPBA, a necessidade de seu destaque, se cabível, bem como a discriminação das informações requeridas nas Notas Fiscais, conforme os comandos legais específicos;

11.14 Responsabilizar-se pelos vícios, ainda que ocultos, e danos decorrentes da execução do objeto, bem como por todo e qualquer dano causado à Administração ou terceiros, não reduzindo essa responsabilidade a fiscalização ou o acompanhamento da execução contratual pelo MPBA, que ficará autorizado a descontar dos pagamentos devidos ou da garantia, caso exigida, o valor correspondente aos danos sofridos;

11.15 Atender, nos prazos consignados neste instrumento, às recusas ou determinações, pelo MPBA, de refazimento dos serviços que não estejam sendo ou não tenham sido executados de acordo com o estipulado neste instrumento, providenciando sua imediata correção, sem ônus para o MPBA;

11.15.1 Comunicar ao MPBA, no prazo de 24 (vinte e quatro) horas, qualquer ocorrência anormal relativa à execução;

11.16 Prestar todo esclarecimento ou informação solicitada pelo MPBA ou por seus prepostos, garantindo-lhes o acesso, a qualquer tempo, aos documentos relativos à execução do objeto;

11.17 Não contratar, durante a vigência do futuro contrato, cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, de dirigente do MPBA, ou do fiscal ou do gestor, nos termos do artigo 48, parágrafo único, da Lei 14.133/2021;

11.18 Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do futuro contrato;

11.19 Cumprir, durante todo o período de execução do futuro contrato, a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, bem como as reservas de cargos previstas na legislação (art. 116, da Lei nº 14.133/2021);

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

11.21 Prestar diretamente os serviços ora contratados, não os transferindo a outrem, no todo ou em parte, sendo vedada a subcontratação, ainda que parcial, do objeto contratado.

CLÁUSULA DÉCIMA SEGUNDA – DAS OBRIGAÇÕES DO CONTRATANTE

12.1 **O CONTRATANTE**, além das obrigações contidas neste contrato por determinação legal, obriga-se a:

12.2 Receber os serviços no prazo e condições estabelecidas no Edital e seus anexos;

12.3 Verificar minuciosamente, no prazo fixado, a conformidade dos serviços recebidos provisoriamente com as especificações constantes do Edital e da proposta, para fins de aceitação e recebimento definitivo;

12.4 Comunicar ao fornecedor, por escrito, sobre imperfeições, falhas ou irregularidades verificadas no objeto fornecido, para que seja refeito, reparado ou corrigido;

12.5 Acompanhar e fiscalizar o cumprimento das obrigações do fornecedor, através de comissão/servidor especialmente designado;

12.6 Efetuar o pagamento ao fornecedor no valor correspondente a execução do objeto, no prazo e forma estabelecidos neste instrumento;

12.7 Rejeitar os serviços executados fora das especificações exigidas ou quando não estejam de conformidade com os padrões de qualidade, dando ciência dos motivos da recusa ao fornecedor, que assumirá todas as despesas daí decorrentes.

12.8 Notificar previamente ao fornecedor, quando da aplicação de penalidades;

12.9 Atestar as notas fiscais/faturas emitidas pelo fornecedor, recusando-as quando inexatas ou incorretas, efetuando todos os pagamentos nas condições pactuadas;

12.10 Emitir Ordem de Serviço para instruir a execução dos serviços;

12.11 Rejeitar, no todo ou em parte, os serviços executados em desacordo com as exigências do Termo de Referência e seus anexos.

12.12 Explicitamente emitir decisão sobre todas as solicitações e reclamações relacionadas à execução do presente Contrato, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do ajuste, observando os seguintes prazos:

12.12.1 A administração responderá à contratada dentro dos prazos legalmente estabelecidos, contados da data da conclusão da instrução do requerimento.

CLÁUSULA DÉCIMA TERCEIRA - DO CUMPRIMENTO DA LEI GERAL DE PROTEÇÃO DE DADOS - LEI N. 13.709/2018

13.1 É vedado às partes a utilização de todo e qualquer dado pessoal repassado em decorrência da execução contratual para finalidade distinta daquela do objeto da contratação, mantendo-se sigilo e confidencialidade, sob pena de responsabilização administrativa, civil e criminal;

13.2 A **CONTRATADA** declara que tem ciência da existência da Lei Geral de Proteção de Dados e se compromete a adequar todos os procedimentos internos ao disposto na legislação com o intuito de proteger os dados pessoais repassados pelo **CONTRATANTE**;

13.3 A **CONTRATADA** fica obrigada a comunicar ao **Ministério Público do Estado da Bahia**, em até 24 (vinte e quatro) horas do conhecimento, qualquer incidente de acessos não autorizados aos dados pessoais, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, bem como adotar as providências dispostas no art. 48 da LGPD;

13.4 A **CONTRATADA** cooperará com o **CONTRATANTE** no cumprimento das obrigações referentes ao exercício dos direitos dos titulares previstos na LGPD e nas Leis e Regulamentos de Proteção de Dados em vigor e também no atendimento de requisições e determinações do Poder Judiciário, Ministério Público, ANPD e Órgãos de controle administrativo em geral;

13.5 Eventuais responsabilidades das partes serão apuradas conforme estabelecido neste contrato e também de acordo com o que dispõe a Seção III, Capítulo VI da LGPD.

CLÁUSULA DÉCIMA QUARTA - DA GARANTIA DA EXECUÇÃO

Não será exigida garantia da execução contratual.

CLÁUSULA DÉCIMA QUINTA – DAS INFRAÇÕES E DAS SANÇÕES ADMINISTRATIVAS

15.1 A **CONTRATADA** sujeitar-se-á às sanções administrativas previstas nas Leis Federal nº. 14.133/2021 e Estadual nº 14.634/23, as quais poderão vir a ser aplicadas após o prévio e devido processo administrativo, assegurando-lhe, sempre, o contraditório e a ampla defesa;

15.2 Comete infração administrativa, nos termos da Lei nº 14.133, de 2021, a **CONTRATADA** que:

15.2.1 Der causa à inexecução parcial do contrato;

15.2.2 Der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;

15.2.3 Der causa à inexecução total do contrato;

15.2.4 Não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;

15.2.5 Ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;

15.2.6 Apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;

15.2.7 Não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

15.2.8 Praticar ato fraudulento na execução do contrato;

15.2.9 Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

15.2.10 Praticar ato lesivo previsto no art.5º da Lei nº 12.846, de 1º de agosto de 2013;

15.3 Serão aplicadas ao responsável pelas infrações administrativas acima descritas as seguintes sanções:

15.3.1 **Advertência**, quando a **CONTRATADA** der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, §2º, da Lei Federal nº 14.133/2021);

15.3.2 **Impedimento de licitar e contratar**, quando praticadas as condutas descritas nos itens 15.2.2, a 15.2.4 acima, sempre que não se justificar a imposição de penalidade mais grave (art. 156, §4º, da Lei Federal
14.133/2021);

15.3.3 **Declaração de inidoneidade para licitar e contratar**, quando praticadas as condutas descritas nos itens 15.2.5 a 15.2.10, acima, bem como nas alíneas 15.2.2 a 15.2.4, que justifiquem a imposição de penalidade mais grave (art. 156, §5º, da Lei Federal nº 14.133/21);

15.3.4 Multa:

15.3.4.1 Moratória de 0,5% (meio por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 30 (trinta) dias;

15.3.4.2 Compensatória de 20% (vinte por cento) sobre o valor total do contrato, para as infrações descritas nas alíneas 15.2.6 a 15.2.10;

15.3.4.3 Compensatória de 20% (vinte por cento) sobre o valor total do contrato, para as infrações descritas na alínea 15.2.3 e 15.2.4;

15.3.4.4 Para as infrações constantes das alíneas 15.2.1, 15.2.2 e 15.2.5, a multa será de 20% (vinte por cento) sobre o valor total do contrato;

15.3.4.5 Será admitida medida cautelar destinada a garantir o resultado útil do processo administrativo sancionatório, de forma antecedente ou incidental à sua instauração, inclusive a retenção provisória do valor correspondente à estimativa da sanção de multa;

15.3.4.5.1 O valor da retenção provisória a que se refere o subitem anterior deste artigo não poderá exceder ao limite máximo estabelecido no §3º do art. 156 da Lei Federal nº 14.133, de 2021;

15.4 A aplicação das sanções previstas neste Contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao **CONTRATANTE**;

15.5 Todas as sanções previstas neste Contrato poderão ser aplicadas cumulativamente com a multa;

15.5.1. Antes da aplicação da multa será facultada a defesa do interessado no prazo de **15 (quinze) dias úteis**, contado da data de sua intimação;

15.5.2. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo **CONTRATANTE** à **CONTRATADA**, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente, conforme o caso;

15.5.3. Previamente ao encaminhamento à cobrança judicial, a multa poderá ser recolhida administrativamente no prazo máximo de 30 (trinta) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente;

15.6. A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa aa contratada, observando-se o procedimento previsto no caput e parágrafos do art. 158 da Lei nº 14.133, de 2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar;

15.7. Na aplicação das sanções serão considerados:

15.7.1 A natureza e a gravidade da infração cometida;

15.7.2 As peculiaridades do caso concreto;

15.7.3 As circunstâncias agravantes ou atenuantes;

15.7.4 Os danos que dela provierem para o **CONTRATANTE**;

15.7.5 A implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle;

15.8 Os atos previstos como infrações administrativas na Lei nº 14.133, de 2021, e na Lei Estadual nº 14.634/23, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846, de 2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei;

15.9 A personalidade jurídica da contratada poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Contrato ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com a contratada, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia;

15.10 O **CONTRATANTE** deverá, no prazo máximo 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ela aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no Cadastro Nacional de Empresas Punidas (Cnep), instituídos no âmbito do Poder Executivo Federal;

15.11 As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133/21 e da Lei Estadual de nº 14.634/23;

15.12 Os débitos da contratada para com a Administração contratante, resultantes de multa administrativa e/ou indenizações, não inscritos em dívida ativa, poderão ser compensados, total ou parcialmente, com os créditos devidos pelo referido órgão decorrentes deste mesmo contrato ou de outros contratos administrativos que a contratada possua com o mesmo órgão ora contratante.

CLÁUSULA DÉCIMA SEXTA – DAS ALTERAÇÕES CONTRATUAIS

16.1 Eventuais alterações contratuais reger-se-ão pela disciplina dos arts. 124 e seguintes da Lei nº 14.133, de 2021 e da Lei Estadual de n º 14.634/23;

16.2 A **CONTRATADA** é obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato;

16.3 As alterações contratuais deverão ser promovidas mediante celebração de termo aditivo, submetido à prévia análise da Assessoria Jurídica do **CONTRATANTE**, salvo nos casos de justificada necessidade de antecipação de seus efeitos, hipótese em que a formalização do aditivo deverá ocorrer no prazo máximo de 1 (um) mês;

16.4 Registros que não caracterizem alteração do contrato podem ser realizados por simples apostila, dispensada a celebração do termo aditivo, na forma do artigo 136, da Lei 14.133, de 2021.

CLÁUSULA DÉCIMA SÉTIMA – DA EXTINÇÃO DO CONTRATO

17.1 O contrato se extingue quando vencido o prazo nele estipulado, independentemente de terem sido cumpridas ou não as obrigações de ambas as partes contraentes;

17.1.1. O contrato pode ser extinto antes do prazo nele fixado, sem ônus para o **CONTRATANTE**, quando este não dispuser de créditos orçamentários para sua continuidade ou quando entender que o contrato não mais lhe oferece vantagem;

17.1.1.2. A extinção nesta hipótese ocorrerá na próxima data de aniversário do contrato, desde que haja a notificação da contratada pelo **CONTRATANTE** nesse sentido com pelo menos 2 (dois) meses de antecedência desse dia;

17.1.1.3. Caso a notificação da não-continuidade do contrato de que trata este subitem ocorra com menos de 2 (dois) meses da data de aniversário, a extinção contratual ocorrerá após 2 (dois) meses da data da comunicação;

17.2 O contrato pode ser extinto antes de cumpridas as obrigações nele estipuladas, ou antes do prazo nele fixado, por algum dos motivos previstos no artigo 137 da Lei Federal nº 14.133/2021, bem como de forma consensual, assegurados o contraditório e a ampla defesa;

17.2.1 A extinção do contrato poderá ser:

a) determinada por ato unilateral e escrito da Administração, exceto no caso de descumprimento decorrente de sua própria conduta (arts. 138, inciso I, da Lei nº 14.133, de 2021);
b) consensual, por acordo entre as partes, por conciliação, por mediação ou por comitê de resolução de disputas, desde que haja interesse da Administração (art. 138, inciso II, da Lei nº 14.133, de 2021);
c) determinada por decisão arbitral, em decorrência de cláusula compromissória ou compromisso arbitral, ou por decisão judicial (art. 138, inciso III, da Lei nº 14.133, de 2021);

17.2.2 A alteração social ou modificação da finalidade ou da estrutura da empresa não ensejará rescisão se não restringir sua capacidade de concluir o contrato;

17.2.2.1 Se a operação implicar mudança da pessoa jurídica **CONTRATADA**, deverá ser formalizado termo aditivo para alteração subjetiva;

17.3 O termo de rescisão, sempre que possível, será precedido:

17.3.1 Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

17.3.2 Relação dos pagamentos já efetuados e ainda devidos;

17.3.3 Indenizações e multas.

17.4 O contrato poderá ser extinto, ainda:

17.4.1 Caso se constate que a contratada mantém vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade **CONTRATANTE** ou com agente público que tenha desempenhado função na licitação no processo de contratação direta ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau;

17.4.2 Caso se constate que a pessoa jurídica **CONTRATADA** possui administrador ou sócio com poder de direção, familiar de detentor de cargo em comissão ou função de confiança que atue na área responsável pela demanda ou contratação ou de autoridade a ele hierarquicamente superior no âmbito do órgão **CONTRATANTE**.

CLÁUSULA DÉCIMA OITAVA – DA PUBLICIDADE

O CONTRATANTE será responsável pela publicação deste instrumento nos termos e condições previstas na Lei nº 14.133/2021.

CLÁUSULA DÉCIMA NONA – 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 VIGÉSIMA – DAS DISPOSIÇÕES GERAIS

20.1 **O CONTRATANTE** não responderá por quaisquer compromissos assumidos perante terceiros pela **CONTRATADA**, ou seus prepostos, ainda que vinculados à execução do presente Contrato;

20.2 A inadimplência da **CONTRATADA**, com relação a quaisquer custos, despesas, tributos, exigências ou encargos, não transfere ao **CONTRATANTE** a responsabilidade pelo seu pagamento, nem poderá onerar o objeto do contrato;

20.3 Os casos omissos serão decididos pelo **CONTRATANTE**, segundo as disposições contidas na Lei Federal nº 14.133, de 2021 e estadual nº 14.634 de 2023 e demais normas federais e estaduais aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei nº 12.078, de 1990 – Código de Defesa do Consumidor – e normas e princípios gerais dos contratos;

20.4 Fica assegurado ao **CONTRATANTE** o direito de alterar unilateralmente o Contrato, mediante justificativa expressa, nas hipóteses previstas na Lei Federal 14.133/21 e na forma de Lei Estadual de nº 14.634/23 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**;

20.5 Não caracterizam novação eventuais variações do valor contratual resultantes de reajustamento/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;

20.6 A Administração não responderá por quaisquer compromissos assumidos pela **CONTRATADA** com terceiros, ainda que vinculados à execução do contrato, bem como por qualquer dano causado a terceiros em decorrência de ato da **CONTRATADA**, de seus empregados, prepostos ou subordinados;

20.7 O presente contrato regula-se pelas suas cláusulas e pelos preceitos de direito público, aplicando-se, supletivamente, os princípios da teoria geral dos contratos e as disposições de direito privado;

E, por assim estarem justos e acordados, assinam o presente Contrato para que produza seus efeitos legais.

Salvador, 2025.

Centro de Pesquisas em Informática Ltda
João Gualberto Rizzo Araújo
sócio - administrador
MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA
André Luis Sant´Ana Ribeiro
Superintendente de Gestão Administrativa

(Assinado e datado eletronicamente/digitalmente)

APENSO I
ESPECIFICAÇÕES TÉCNICAS DETALHADAS

OBJETO: Contratação de Serviço Gerenciado de Soluções de Segurança para proteção dos dispositivos, estações de trabalho e servidores, incluindo capacidade estendida de prevenção, detecção e resposta, acesso remoto seguro, gestão de vulnerabilidades, visibilidade, garantias de conformidade, controle de acesso e automação, não apenas para os dispositivos, mas também para os usuários, bem como serviços de instalação, treinamento, gerenciamento, manutenção e atualização das soluções, garantias de conformidade e resposta a incidentes para a equipe do Ministério Público da Bahia em regime 24x7 com atendimento on-site, conforme detalhamento descrito neste documento de especificações técnicas detalhadas, pelo período de 36 meses.

ESPECIFICAÇÕES TÉCNICAS:

1. Item 1 – Serviços Gerenciados de Soluções de Segurança para plataforma SSE com controle de acesso remoto, pelo período de 36 meses

1.1. A plataforma de segurança a ser fornecida na modalidade Software como Serviço (SaaS), deve possuir alinhamento direto com o conceito Security Service Edge do Gartner, mais especificamente para funcionalidade de Acesso remoto seguro: Redirecionamento seguro baseado no conceito Zero Trust Network Access para as aplicações internas posicionadas no ambiente on-premise ou em nuvens públicas.

1.2. CARACTERÍSTICAS GERAIS

1.3. A solução de segurança proposta deverá ser fornecida em uma arquitetura 100% baseada em nuvem.

1.4. O fabricante deverá prover, no mínimo, 3 (três) estruturas de processamento de dados no Brasil para melhor experiência do usuário, garantindo:

1.4.1 Uso global, com mais de 50 pontos no mundo, da infraestrutura do fabricante;

1.4.2 Uso irrestrito de banda por parte dos usuários;

1.4.3 Disponibilidade de 99.999% dos datacenters no Brasil e no mundo;

1.4.4 30 ms para tráfego não criptografado e 70 ms para tráfego criptografado;

1.4.5 Armazenamento de eventos no período mínimo de 90 dias;

1.4.6 Deverá prover 90 dias de retenção de logs na console administrativa;

1.5. O fabricante deverá prover suporte nativo ao Microsoft Active Directory (ADFS) e Microsoft Azure AD (SCIM e SAML v2), para:

1.5.1 Autenticação dos usuários para o Acesso Remoto;

1.5.2 Sincronização de usuários, grupos e OU’s;

1.5.3 Single Sign-on para usuários administrativos.

1.6. Os dados dos usuários do MPBA deverão ser logicamente apartados através de arquitetura multi-tenant ofertada pela plataforma;

1.7. Toda inspeção do tráfego deverá ser feita em nuvem, com exceção das exceções de tráfego local e conformidade do dispositivo;

1.8. A solução deverá prover painel único de gestão, contemplando os módulos propostos neste referencial técnico.

1.9. O agente do próprio fabricante, instalado no dispositivo do usuário deverá avaliar a postura do dispositivo, liberando ou não o acesso as aplicações baseando-se na identificação de itens, como:

1.9.1 Processo em execução;

1.9.2 Presença de arquivos armazenados em disco local;

1.9.3 Presença de um domínio Windows;

1.9.4 Presença de um certificado digital no dispositivo.

1.10. Deverá atuar como um roteador em nuvem, garantindo baixa latência e canal seguro, para aplicações privadas do MPBA;

1.11. Será permitida a inclusão de um appliance físico ou virtual na infraestrutura do MPBA para a comunicação segura entre nuvem do fabricante e servidores internos;

1.12. A solução deverá fornecer o acesso à aplicação apenas, não ao contexto de rede;

1.13. Deverá permitir o redirecionamento seguro para pelo menos 800 (oitocentas) aplicações internas;

1.14. Deverá ser capaz de autorizar o acesso ou não a aplicações internas baseada no perfil da máquina;

1.15. Deverá ser capaz de continuamente solicitar ao usuário que autentique novamente antes de ter acesso às aplicações privadas;

1.16. O acesso deve ser dedicado e exclusivo a aplicação designada na rede, não sendo permitido acesso irrestrito a um host ou a rede;

1.17. A solução de ZTNA deverá prover acesso seguro e controlado baseado nos protocolos TCP e UDP a aplicações privadas da MPBA através de cliente do próprio fabricante instalado na máquina;

1.18. A solução deverá suportar aplicações legadas baseadas em arquitetura cliente - servidor, operadas sob protocolos TCP/UDP.

1.19. Deverá prover acesso a pelo menos as seguintes aplicações:

1.19.1 SSH - TCP Porta 22;

1.19.2 HTTP - TCP Portas 80, 443 e Customizadas;

1.19.3 RDP - TCP 3389 e UDP 3389;

1.19.4 SQL Server - TCP 1333, 1434 | UDP 1434;

1.19.5 SMB - TCP 445;

1.19.6 FTP - TCP 21.

1.20. O acesso seguro as aplicações definidas poderão ser restritas, no mínimo, para:

1.20.1 Usuário Único;
1.20.2 Múltiplos Usuários;

1.20.3 Grupos de Usuário;

1.20.4 Unidade Organizacional (OU).

1.21. Para cada acesso, a política deverá prover múltiplas possibilidades de ações, dentre elas:

1.21.1 Permitir;

1.21.2 Bloquear.

1.22. Deve ser possível determinar apenas o endereço IP e porta de acesso da aplicação sem a necessidade de determinar um segmento de rede interno que o usuário remoto terá acesso;

1.23. Ao se conectar remotamente na solução para acesso a uma aplicação interna, a máquina remota não deve ter acesso, nem ser atribuído em um segmento de rede interna como em um sistema de VPN tradicional;

1.24. Deverá ser capaz de continuamente solicitar ao usuário que autentique novamente antes de ter acesso às aplicações privadas em um iDP externo (Microsoft azure AD).

1.25. A solução deverá prover o monitoramento de comportamento de usuário para identificar possíveis violações no acesso a aplicações web privadas.

1.26. A solução deverá suportar a importação de usuários a partir do Microsoft Active Directory.

1.27. A solução de segurança deverá suportar função Pre-Logon para plataformas Microsoft.

1.28. A solução deverá prover acesso a aplicações Web (HTTPS) sem a necessidade de instalação de agentes.

1.29. A solução deverá prover capacidade de avaliação contínua do endpoint para avaliação das validações de conformidade.

1.30. Deverá permitir o acesso diferenciado para um mesmo usuário conforme as seguintes condições:

1.30.1 Máquinas em conformidade: A partir de uma máquina gerenciada, com pré-requisitos de segurança identificados, deve permitir o acesso à aplicação.

1.30.2 Máquinas não conformes: A partir de uma máquina gerenciada, uma estação que não atenda aos requisitos de segurança, deve bloquear o acesso à aplicação.

1.31. CONSOLE DE GESTÃO CENTRALIZADA

1.32. A solução deverá possuir capacidade de gestão centralizada, mantendo um painel único de visibilidade para todos os módulos descritos neste termo de referência.

1.33. Toda a parte de gestão deverá ser centralizada em uma única console, garantindo a aplicação das políticas criadas em todos os pontos de presença disponíveis pelo fabricante e independente de qual data center o usuário faça uso, a política estará vigente para proteção e controle do tráfego.

1.34. Todos os dados disponíveis para a consulta e criação de relatórios, deverão residir na console de gestão por 90 dias.

1.35. A plataforma deve permitir a criação de diferentes perfis de acesso a console de administração com, no mínimo, as seguintes possibilidades:

1.35.1 Perfil de administrador geral: acesso total às funções da solução, acesso aos logs de auditoria dos outros usuários, criação e administração de outras contas de acesso;

1.35.2 Perfil de administrador intermediário: acesso total às funções da solução, exceto criação e administração de outras contas de acesso.

2.Item 2 – Serviços Gerenciados de Gestão de Exposição Cibernética por 36 meses

2.1 A solução deve realizar varreduras (scans) de vulnerabilidades, avaliação de configuração e conformidade (baseline e compliance);

2.2. A solução deve possuir recurso de varredura ativa, onde o scanner comunica-se com os alvos (ativos) através da rede;

2.3. A solução de gestão de vulnerabilidades deve suportar varreduras de dispositivos de IoT;

2.4. A solução deve ser licenciada pelo número de endereços IP ou dispositivos (assets);

2.5. A solução deve fornecer um modelo de armazenamento integrado que não dependa de um banco de dados externos ou de terceiros;

2.6. Caso a solução dependa de banco de dados de terceiros, todas as licenças deverão ser fornecidas pela **CONTRATADA**.

2.8. A solução deverá suportar API (Application Programming Interface) baseada em REST (Representatonal State Transfer) para automação de processos e integração com aplicações terceiras.

2.9 A solução deve possuir integração via API no mínimo as seguintes linguagens: Python, Powershell, Ruby, javascript, Java, Swift e PHP; A solução deve possuir métodos de consulta via api e envio, tais como: HTTP METHOD (POST, GET, PUT AND DELETE);

2.10. A solução deve incluir a opção para agentes instalados e licenciados em estações de trabalho e servidores, para varredura diretamente no sistema operacional;

2.11. Tais agentes devem ser gerenciados pela mesma interface/console da plataforma de gestão de vulnerabilidades;

2.12. A solução deve permitir o agrupamento de scanners para facilitar o gerenciamento e aplicação de políticas;

2.13. A solução deve realizar a varredura tanto de dispositivos na rede interna, dispositivos expostos a demais redes externas, tanto quanto dispositivos em nuvens públicas como Azure, AWS ou GCP;

2.14. O escaneamento para os dispositivos expostos deve sem realizados através de SCANS (ENGINE) do próprio fabricante alocados no Brasil;

2.15. Os scanners e sensores agentes deverão ser gerenciados por uma única plataforma, de maneira
centralizada;

2.16. O acesso a console de gerenciamento deve ser fornecida para pelo menos 10 usuários simultâneos;

2.17. A solução deve ser capaz de se integrar e disponibilizar insumos para soluções de correlação de eventos externa (SIEM);

2.18. A solução deve apresentar, para cada vulnerabilidade encontrada, a descrição e passos que devem ser tomados para correção;

2.19. A solução deve apresentar, para cada vulnerabilidade encontrada, evidências da vulnerabilidade através de saídas das verificações (outputs);

2.20. A solução deve fornecer controle de acesso baseado em função (RBAC- Role Based Access Control) para controlar o acesso do usuário a conjuntos de dados e funcionalidades;

2.21. A solução deve ser capaz de definir e gerenciar grupos de usuários, incluindo limitação de funções de varreduras e acesso a relatórios e dashboards;

2.22. A solução deve ter a capacidade de excluir determinados endereços IP do escopo de qualquer varredura ou scan;

2.23. A solução deve criptografar todos resultados de varreduras obtidos e informações inseridas tanto em descanso quanto em trânsito;

2.24. A solução deve suportar métodos de autenticação usando bases de autenticação local, e SAML (Security
Assertion Markup Language) para uso de SSO (Single SignOn);

2.25. A solução deve ser capaz de orquestrar scanners ilimitados dentro da infraestrutura;

2.26. A solução não deve impor nenhum limite de quantidade de scanners implementados dentro da infraestrutura;

2.27. A solução deverá possuir sistema de alertas para informar a disponibilidade de resultados dos escaneamentos através de email;

2.28. A solução deve oferecer capacidade de configuração dinâmica de grupos de ativos através de no mínimo as seguintes características:

2.29. Sistema Operacional, Endereço IP, DNS, NetBIOS Host, MAC, AWS Instance Type, AWS EC2 Name, Software instalado, Azure VM ID, AWS Region, Google Cloud Instance ID, Azure Resource ID, Ativos avaliados;
2.30. DOS RELATÓRIOS E PAINÉIS GERENCIAIS

2.31. A solução deverá possuir painéis gerenciais (dashboards) pré-definidos para rápida visualização dos resultados, permitindo ainda a criação de painéis personalizados;

2.32. Os painéis gerenciais deverão ser apresentados em diversos formatos, incluindo gráficos e tabelas, possibilitando a exibição de informações em diferentes níveis de detalhamento;

2.33. Os relatórios devem ser disponibilizados sob demanda no console de gerência da solução;

2.34. Os relatórios devem conter informações da vulnerabilidade, severidade, se existe um exploit disponível e informações do ativo;

2.35. A solução deve permitir a customização de dashboards/relatórios;

2.36. A solução deve concentrar todos os relatórios na plataforma central de gerenciamento, não sendo aceitas soluções fragmentadas;

2.37. A solução deve ser capaz de produzir relatórios, pelo menos, nos seguintes formatos: HTML, PDF e CSV;

2.38. A solução deve possibilitar a criação de relatórios baseado nos seguintes alvos: Todos os ativos e Alvos específicos;

2.39. Deve suportar a criação de relatórios criptografados (protegidos por senha configurável);

2.40. A solução deve suportar o envio automático de relatórios para destinatários específicos;

2.41. Deve ser possível definir a frequência na geração dos relatórios para no mínimo: Diário, Mensal, Semanal e Anual;

2.42. Permitir especificar níveis de permissão nos relatórios para usuários e grupos específicos;

2.43. DAS VARREDURAS

2.44. A solução deve realizar varreduras em uma variedade de sistemas operacionais, incluindo no mínimo Windows, Linux e Mac OS, bem como appliances virtuais;

2.45. A solução deve suportar varredura com e sem agente, de maneira ativa e passiva, distribuídas em diferentes localidades e regiões e gerenciar todos por uma console central;

2.46. A solução deve fornecer agentes instaláveis em sistemas operacionais distintos para monitoramento contínuo de vulnerabilidades;

2.47. Tais agentes devem realizar conexões para o sistema gerenciamento através de protocolo seguro;

2.48. A solução deve ser configurável para permitir a otimização das configurações de varredura;

2.49. A solução deve permitir a entrada e o armazenamento seguro de credenciais do usuário, incluindo contas locais, de domínio (LDAP e Active Directory) e root para sistemas Linux;

2.50. A solução deve fornecer a capacidade de escalar privilégios nos destinos, do acesso de usuário padrão até acesso de sistema ou administrativo;

2.51. A solução deve se integrar com solução de gerenciamento de acessos privilegiados para autenticação nos dispositivos, no mínimo, os seguintes:

2.52. CyberArk;

2.53. BeyondTrust;

2.54. Thycotic;

2.55. Centrify;

2.56. A solução deve suportar o agendamento de scans personalizados, incluindo a capacidade de executar varreduras em tempos designados, com frequência pré-determinada;

2.57. A solução deve ser capaz de identificar novos hosts no ambiente sem a necessidade de scan;

2.58. A solução deve possuir recurso de monitoria passiva do tráfego de rede para identificação de anomalias, novos dispositivos e desvios de padrões observados;

2.59. A solução deve ser capaz de realizar em tempo real a descoberta de vulnerabilidades nas seguintes tecnologias:
2.60. Cloud Services;

2.61. Data Leakage;

2.62. Database;

2.63. IoT;

2.64. Mobile Devices;

2.65. Operating System;

2.66. Peer-To-Peer;

2.67. SCADA;

2.68. Web Servers;

2.69. Web Clients;

2.70. A solução deve ser capaz de identificar a comunicação de malwares na rede de forma passiva;

2.71. A solução deve em tempo real, detectar logins e downloads de arquivos em um compartilhamento de rede;

2.72. DA ANÁLISE E PRIORIZAÇÃO DE VULNERABILIDADES

2.73. A solução deve ser capaz de exibir ambos severidade e pontuação, com base em CVSS (Common Vulnerability Scoring System) e inteligência de ameaças;

2.74. A solução deve utilizar sistema de pontuação e priorização das vulnerabilidades que utilize no mínimo:

2.75. CVSS Impact Score;

2.76. Idade da Vulnerabilidade;

2.77. Maturidade de códigos de exploração da vulnerabilidade encontrada;

2.78. Frequência de uso da vulnerabilidade em ataques e campanhas atuais;

2.79. Disponibilidade do código de exploração da vulnerabilidade;

2.80. Presença de módulos de exploração de vulnerabilidade em frameworks automatizados de exploração de vulnerabilidades como CANVAS, Metasploit e Core Impact;

2.81. Popularidade da vulnerabilidade em fóruns e comunicações na Darkweb;

2.82. O mecanismo de priorização deve ser sujeito a modificações e atualizações diárias com base em inteligência de ameaças e observação de tendências na Internet;

2.83. DA ANÁLISE DE RISCO DO AMBIENTE

2.84. A solução deve gerar um score que combine dados de vulnerabilidades com a criticidade dos ativos do ambiente computacional;

2.85. O score deve ser gerado automaticamente por meio de algoritmos de inteligência artificial (Machine Learning) e deve calcular a probabilidade de exploração de uma determinada vulnerabilidade;

2.86. Deve ser capaz de calcular a criticidade dos ativos da organização;

2.87. A solução deve ser capaz de realizar um benchmark no ambiente do **CONTRATANTE** comparando sua maturidade com outras organizações do mesmo setor;

2.88. A solução deve prover visão sobre quais ações de remediação reduzem o maior nível de risco do ambiente;

2.89. A solução deve também permitir a visualização de ações de remediação agregadas para visão consolidada de redução de risco;

2.90. Deve permitir modificar a qualquer momento o tipo de indústria para comparação. Ex: Mudar de Setor Público para Mercado Financeiro;

2.91. Deve fornecer uma lista com as principais recomendações para o ambiente com foco na redução da exposição cibernética da organização;

2.92. A solução deve gerar uma pontuação para cada um dos ativos onde é levado em conta as vulnerabilidades presentes naquele ativo assim como a classificação do ativo na rede (peso do ativo);

2.93. A solução deve gerar uma pontuação global referente a exposição cibernética da organização baseado nas pontuações de cada um dos ativos;

2.94. A solução deve oferecer uma capacidade de comparação (benchmarking) da pontuação referente a exposição cibernética com outros players da mesma indústria assim como outras empresas do mercado;

2.95. A solução deve permitir um acompanhamento histórico do nível de exposição da organização;

2.96. Permitir realizar alterações na classificação dos ativos (atribuição de pesos diferentes) podendo sobrescrever a classificação atribuída automaticamente pela solução;

2.97. A solução deverá apresentar indicadores específicos referentes a remediação, possuindo no mínimo informações referentes ao tempo entre remediação e o tempo o qual a vulnerabilidade foi descoberta no ambiente, tempo entre a remediação e a data de publicação da vulnerabilidade, quantidade média de vulnerabilidades críticas por ativo e a comparação da quantidade de vulnerabilidades corrigidas por criticidade;

2.98. A solução deve permitir a segregação lógica entre áreas distintas da empresa afim de obter a pontuação referente exposição cibernética por área;

2.99. DO GERENCIAMENTO DA ANÁLISE DE ATAQUES EXPLORÁVEIS

2.100. Deve disponibilizar visibilidade nas técnicas de ataque baseado no framework MITRE ATT&CK;

2.101. Deve identificar qual a criticidade do ataque, em no mínimo: baixo, médio e alto;

2.102. Deve prover a evidência relacionada a descoberta do ataque;

2.103. Deve mostrar o objeto relacionado ao ataque, de origem e de destino;

2.104. Deve apresentar informações detalhadas relacionadas a mitigação para o ataque em análise;

2.105. Deve prover quais ferramentas e possíveis malwares associados ao ataque;
2.106. Deve disponibilizar de forma gráfica via console de gerenciamento as conexões entre os objetos do ataque;

2.107. Deve disponibilizar uma biblioteca com ‘Queries’ para a busca de objetos no mínimo os seguintes segmentos:

2.108. Rede;

2.109. Endpoint;

2.110. Active Directory;

2.111. Permissão;

2.112. Ransomware;

2.113. Vetores;

2.114. Credenciamento;

2.115. Deve suportar no mínimo 120 técnicas de ataques;

2.116. Deve possuir integração nativas com os módulos de WEB, Vulnerabilidades de Infraestrutura, Active Directory e ambientes em nuvem;

2.117. DA DESCOBERTA DE ATIVOS

2.118. A solução deve ser capaz de realizar escaneamento de descoberta de rede utilizando os seguintes critérios como alvo: IP, CIRD e Range;

2.119. A solução deve disponibilizar modelos de escaneamento de descoberta, ajustável, com os seguintes tipos de scan:

2.120. Enumeração de Hosts;

2.121. Identificação de Sistema Operacional (SO);

2.122. Port Scan (Portas comuns);

2.123. Port Scan (Todas as portas);

2.124. Customizado;

2.125. A solução deve permitir realizar escaneamento de descoberta customizado podendo ser parametrizado de acordo com a necessidade;

2.126. A parametrização do escaneamento de descoberta deve, no mínimo, conter os seguintes requisitos:

2.127. Descoberta de Host;

2.128. Ping o host remoto;

2.129. Usar descoberta rápida;

2.130. Métodos de ping;
2.131. ARP;

2.132. TCP;

2.133. ICMP;

2.134. UDP;

2.135. Escaneamento de descoberta de dispositivos de OT/SCADA;

2.136. Escaneamento de descoberta em redes de impressora;

2.137. Escaneamento em redes Novell;

2.138. Tecnologia de Wake-on-LAN;

2.139. Port Scanning:

2.140. Portas;

2.141. Considerar portas não escaneadas como fechadas;

2.142. Range de portas a serem escaneadas;

2.143. Enumerar Portas locais:

2.144. SSH (netstat);

2.145. WMI (netstat);

2.146. SNMP;

2.147. Descoberta de Serviços:

2.148. Sondar todas as portas para encontrar serviços;

2.149. Procurar por serviços baseado em SSL/TLS;

2.150. Enumerar todas as cifras SSL/TLS;

2.151. A solução deve realizar descoberta de ativo de forma passiva e adicionado automaticamente na console de gerenciamento;

2.152. A solução deve descobrir passivamente quando um host é adicionado na rede;

2.153. DA AVALIAÇÃO DE VULNERABILIDADE

2.154. A solução deve ser capaz de realizar testes sem a necessidade de agentes instalados no dispositivo destino para detecção de vulnerabilidades;

2.155. A solução deve detectar e classificar através de severidades, riscos e vulnerabilidades;

2.156. A solução deve também fornecer informações detalhadas sobre a natureza da vulnerabilidade, evidências da existência da vulnerabilidade e recomendações para mitigá-los;
2.157. A solução deve incluir uma saída detalhada das vulnerabilidades descobertas como versões de DLL esperadas e encontradas;

2.158. A solução deve ser compatível com CVE e fornecer pelo menos 10 anos de cobertura CVE;

2.159. A solução deve identificar vulnerabilidades especificas para o Active Directory com os seguintes padrões de verificação;

2.160. Contas administrativas vulneráveis a Kerberoasting attack;

2.161. Utilização de criptografia vulnerável com autenticação Kerberos;

2.162. Contas com pré-autenticação do Kerberos desabilitada;

2.163. Verificação de usuários com a opção de nunca expirar a senha com a opção habilitada;

2.164. Verificar validação de fragilidades do tipo “Unconstrained Delegation”;

2.165. Verificação de “Pre-Windows 2000 Compatible Access”;

2.166. Verificação de validade de chaves mestras "Kerberos KRBTGT”;

2.167. Verificação de “SID History Injection”;

2.168. Verificação de “Printer Bug Exploit”;

2.169. Verificação de “Primary Group ID”;

2.170. Verificação de usuários com Passwords em branco;

2.171. A solução deve suportar o uso de SMB e WMI para verificação de sistemas Microsoft Windows;

2.172. A solução deve ser capaz de iniciar automaticamente serviços de registro remoto em sistemas Windows ao executar uma varredura credenciada;

2.173. A solução deve ser capaz de parar automaticamente o serviço de registro remoto em sistemas Windows novamente assim que a varredura estiver completa;

2.174. O scanner deve oferecer suporte a shell seguro (SSH) com a capacidade de escalar privilégios para varredura de vulnerabilidades e auditorias de configuração em sistemas Unix;

2.175. A solução deve suportar o uso do netstat (Linux) e WMI (Windows) para uma enumeração rápida e precisa de portas em um sistema quando as credenciais são fornecidas;

2.176. A solução deve possibilitar a verificação remota de portas, além da enumeração local de portas, para ajudar a determinar se algum mecanismo de controle de acesso está sendo utilizado;

2.177. A solução deve fornecer auditoria de patch (MS Bulletins) para as principais versões de Windows;

2.178. A solução deve fornecer auditoria de patch para todos os principais sistemas operacionais Unix incluindo Mac OS, Linux, Solaris e IBM AIX;

2.179. A solução deve fornecer varredura para aplicativos comerciais diversos e proprietários, incluindo, mas não limitando-se a: Java, Adobe, Oracle, Apple, Microsoft, Check Point, Palo Alto Networks, Cisco, Fortinet, Fireeye, McAfee, etc;

2.180. A solução deve incluir classificação de severidades de acordo com o padrão Sistema Comum de Pontuação de Vulnerabilidade Versão (CVSS2 e CSVSS 3);

2.181. A solução deve fornecer informações acerca da disponibilidade de códigos de exploração das vulnerabilidades encontradas em frameworks de exploração para as plataformas mais populares: Core, Metasploit e Canvas;

2.182. A solução deve informar se a vulnerabilidade pode e está sendo ativamente explorada por código malicioso (malware);

2.183. A solução deve possuir importação de arquivos .YARA;

2.184. Deve ser capaz de identificar e classificar vulnerabilidades de máquinas virtuais em nuvem pública em infraestruturas como serviço nas plataformas AWS, Microsoft Azure e Google Cloud;

2.185. DA AUDITORIA DE CONFIGURAÇÃO

2.186. A solução deve ser capaz de realizar auditoria de conformidade sem a necessidade de agente instalado no dispositivo de destino;

2.187. A solução deve fornecer benchmarks de auditoria de segurança e configuração para conformidade regulatória e outros padrões de práticas recomendadas pela área ou fabricantes;

2.188. A solução deve realizar verificações de auditoria contendo as de segurança, com indicação de sucesso ou falha, baseado nos principais frameworks reconhecidos pela indústria, pelo menos os seguintes:

2.189. Center for Internet Security Benchmarks (CIS);

2.190. Defense Information Systems Agency (DISA) STIGs;

2.191. Health Insurance Portability and Accountability Act (HIPAA);

2.192. Payment Card Industry Data Security Standards (PCI DSS);

2.193. A solução deve fornecer auditoria de programas antivírus para determinação de presença e status de inicialização para no mínimo os seguintes produtos: TrendMicro Office Scan, McAfee VirusScan, Microsoft Endpoint Protection e Kaspersky;

2.194. A solução deve fornecer auditorias de configuração com base benchmarks em CIS (Center for Internet
Security) L1 e L2, para ambos os sistemas operacionais Microsoft Windows e Linux;

2.195. A solução deve permitir auditoria de conformidade em servidores Windows, Linux, Bancos de Dados SQL Server, a fim de determinar se estão configurados de acordo com os principais Framework de segurança como, por exemplo, CIS e DISA;

2.196. A solução deve oferecer validação e suporte a SCAP (Security Content Automation Protocol);

2.197. DA ANÁLISE DINÂMICA DE VULNERABILIDADES PARA APLICAÇÕES WEB

2.198. A solução deve ser capaz de analisar, testar e reportar falhas de segurança em aplicações Web como parte dos ativos a serem inspecionados;

2.199. A solução deve ser capaz de executar varreduras em sistemas web através de seus endereços IP ou FQDN (DNS);
2.200. A solução deve avaliar no mínimo os padrões de segurança OWASP Top 10 e PCI (payment card industry data security standard);

2.201. A solução deve suportar as diretivas PCI ASV 5.5 para definição de escopo de análise da aplicação;

2.202. A solução deve suportar as diretivas PCI ASV 6.1 para definição de balanceadores de carga das aplicações bem como suas configurações para inclusão no relatório de resultados;

2.203. A solução deve possuir templates prontos de varreduras entre simples e extensos;

2.204. Para varreduras extensas e detalhadas, deve varrer e auditar no mínimo os seguintes elementos:

2.205. Cookies, Headers, Formulários e Links;

2.206. Nomes e valores de parâmetros da aplicação;

2.207. Elementos JSON e XML;

2.208. Elementos DOM;

2.209. A solução deve permitir somente a execução da função crawler, que consiste na navegação para descoberta das URLs existentes na aplicação;

2.210. A solução deve ser capaz de utilizar scripts customizados de crawl com parâmetros definidos pelo usuário;

2.211. A solução deve excluir determinadas URLs da varredura através de expressões regulares;

2.212. A solução deve excluir determinados tipos de arquivos através de suas extensões;

2.213. A solução deve instituir no mínimo os seguintes limites:

2.214. Número máximo de URLs para crawl e navegação;

2.215. Número máximo de diretórios para varreduras;

2.216. Número máximo de elementos DOM;

2.217. Tamanho máximo de respostas;

2.218. Limite de requisições de redirecionamentos;

2.219. Tempo máximo para a varredura;

2.220. Número máximo de conexões HTTP ao servidor hospedando a aplicação Web;

2.221. Número máximo de requisições HTTP por segundo;

2.222. A solução deve detectar congestionamento de rede e limitar os seguintes aspectos da varredura:

2.223. Limite em segundos para timeout de requisições de rede;

2.224. Número máximo de timeouts antes que a varredura seja abortada;

2.225. A solução deve agendar a varredura e determinar sua frequência entre uma única vez, diária, semanal, mensal e anual;
2.226. A solução deve enviar notificações através de no mínimo E-mail e SMS;

2.227. A solução deve possuir a flexibilidade de selecionar quais testes serão realizados de forma granular, através da seleção de testes, plug-ins ou ataques;

2.228. A solução deve avaliar sistemas web utilizando protocolos HTTP e HTTPs;

2.229. A solução deve possibilitar a definição de atributos no cabeçalho (HEADER) da requisição HTTP de forma personalizado a ser enviada durante os testes;

2.230. A solução deve ser compatível com avaliação de web services REST e SOAP;

2.231. Deverá suportar no mínimo os seguintes esquemas de autenticação:

2.232. Autenticação básica (digest);

2.233. NTLM;

2.234. Form de login;

2.235. Autenticação de Cookies;

2.236. Autenticação através de Selenium;

2.237. Autenticação através de Bearer;

2.238. A solução deve importar scripts de autenticação selenium previamente configurados pelo usuário;

2.239. A solução deve customizar parâmetros Selenium como delay de exibição da página, delay de execução de comandos e delay de comandos para recepção de novos comandos;

2.240. A solução deve exibir os resultados das varreduras em tendência temporal para acompanhamento de correções e introdução de novas vulnerabilidades;

2.241. A solução deve exibir os resultados agregados de acordo com as categorias do OWASP Top 10 gory:OWASP_Top_Ten_Project); (https://www.owasp.org/index.php/Cate

2.242. Os resultados devem ser apresentados agregados por vulnerabilidades ou por aplicações;

2.243. Para cada vulnerabilidade encontrada, deve ser exibido evidências da mesma em seus detalhes;

2.244. Para vulnerabilidades de injeção de código (SQL, XSS, XSRF, etc.), deve evidenciar nos detalhes do evento encontrado:

2.245. Payload injetado;

2.246. Evidência em forma de resposta da aplicação;

2.247. Detalhes da requisição HTTP;

2.248. Detalhes da resposta HTTP;

2.249. Os detalhes das vulnerabilidades devem conter descrição da falha e referências didáticas para a revisão dos analistas;

2.250. Cada vulnerabilidade encontrada deve conter também soluções propostas para mitigação ou remediação das mesmas;

2.251. A solução deve possuir suporte a varreduras de componentes para no mínimo:

2.252. Wordpress, Blog Designer Plugin for Wordpress, Event Calendar Plugin for Wordpress, Convert Plus Plugin for Wordpress, AngularJS, Apache, Apache Tomcat, Apache Tomcat JK connecto, Apache Spark e Apache Struts, Atlassian Confluence, Atlassian Crowd e Atlassian Jira, Backbone.js, ASP.NET, Bootstrap, Drupal, Joomla!, jQuery, Lighttpd, Magento, Modernizr, Nginx, PHP, AJAX, Sitefinity, Telerik, ThinkPHP, Webmin e YUI;

2.253. DA ANÁLISE DE RISCO EM AMBIENTE MICROSOFT ACTIVE DIRECTORY

2.254. A solução deve identificar fraquezas ocultas em configurações do dedicadas ao Active Directory;

2.255. A solução deve possuir ações preventivas de hardening para o Active Directory;

2.256. A solução deve identificar ataque específicos para a estrutura do Active Directory;

2.257. A solução deve possuir funcionalidade para analisar em detalhes cada configuração incorreta que acarreta riscos de segurança – com uma linguagem simples, contextualizando tal risco para os times envolvidos;

2.258. A solução deve possuir recomendações de correção para cada configuração incorreta no Active Directory;

2.259. A solução deve avaliar relações de confiança perigosas entre florestas e domínios;

2.260. A solução deve capturar as mudanças que ocorrem no AD e demostrar na console de administração;

2.261. A solução deve possuir dashboard com os principais ataques e vulnerabilidades por domínio;

2.262. A solução deve permitir a correlação de mudanças no Active Directory e desvios de segurança;

2.263. A solução deve analisar em detalhes um ataque explorando as descrições através do framework MITRE ATT&CK;

2.264. A solução deve prover interface web para gerenciamento de todas as funcionalidades;

2.265. A solução deve possuir capacidade nativa de criação de dashboards customizados;

2.266. A solução deve suportar um modelo de controle de acesso baseado em funções (RBAC) flexível;

2.267. A solução deve realizar alterações no Active Directory, seus objetos e atributos;

2.268. A solução deve armazenar ou sincronizar nenhuma credencial de objetos do Active Directory;

2.269. A solução deve suportar ambientes com múltiplas florestas e domínios;

2.270. A solução deve suportar monitoramento contínuo de ambientes com Active Directory com o nível funcional de floresta e domínio a partir do 2003;

2.271. A solução deve suportar reter os eventos coletados por no mínimo um ano;

2.272. A solução deve descobrir e mapear a superfície de ataque do Active Directory e seus domínios monitorados com os seguintes padrões:

2.273. Não depender de agentes ou sensores para coleta de informações do AD;
2.274. A solução deve seguir as boas práticas de menor privilégio, a conta de serviço utilizada para conexão com o Active Directory, sendo o menor nível de acesso esperado para a conta de serviço como parte do grupo Domain User;

2.275. Interface web que consolida e apresenta de maneira unificada os domínios monitorados e as possíveis relações de confiança estabelecidas entre eles;

2.276. A solução deve analisar continuamente a postura de segurança do AD, minimamente avaliando:

2.277. Validação de GPOs desvinculadas, desabilitadas ou órfãs;

2.278. Validação de contas desativadas em grupos privilegiados;

2.279. Domínio usando uma configuração perigosa de compatibilidade com versões anteriores por meio de alterações no atributo dSHeuristics;

2.280. Validação de atributos relacionados a roaming de credenciais vulneráveis (ms-PKIDPAPIMasterKeys) gerenciados por um usuário sem privilégios;

2.281. Validação de domínio sem GPOs de proteção de computador, desativando protocolos vulneráveis antigos, como NTLMv1;

2.282. Validação de contas com senhas que nunca expiram;

2.283. Validação de senhas reversíveis em GPOs;

2.284. Validação de uso de senhas reversíveis em contas de usuário;

2.285. Validação de utilização de protocolo criptográfico fraco (Ex. DES) em contas de usuário; 2.286. Validação de uso do LAPS (Solução de senha de administrador local) para gerenciar senhas de contas locais com privilégios;

2.287. Validação se o domínio possui um nível funcional desatualizado; 2.288. Validação de contas de usuário utilizando senha antiga;

2.289. Validação se o atributo AdminCount está definido em usuários padrão;

2.290. Validação do uso recente da conta de administrador padrão;

2.291. Validação de usuários com permissão para ingressar computadores no domínio;

2.292. Validação de contas dormentes;

2.293. Validação de computadores executando um sistema operacional obsoleto;

2.294. Validação de restrições de logon para usuários privilegiados em ambiente com múltiplos tiers (1, 2 e 3) de segregação de ativos;

2.295. Validação de direitos perigosos configurados no Schema do AD;

2.296. Validação de relação de confiança perigosa com outras Florestas e Domínios;

2.297. Validação de contas que possuem um atributo perigoso de histórico SID (SID History);

2.298. Validação de contas utilizando controle de acesso compatível com versões anteriores ao Windows 2000;

2.299. Validação da última alteração de senha do KDC;

2.300. Validação da última alteração da senha da conta SSO do Azure AD;

2.301. Validação de contas que podem ter senha em branco/vazia;

2.302. Validação de utilização do grupo nativo Protected Users;

2.303. Validação de privilégios sensíveis (Ex. Debug a program, Replace a process level token, etc.) perigosos atribuídos aos usuários;

2.304. Validação de possível senha em clear-text;

2.305. Validação de sanidade das GPOs e componentes CSEs (Client-Side Extension);

2.306. Validação de uso de algoritmos de criptografia fracos na PKI do Active Directory;

2.307. Validação de contas de serviço com SPN (Service Principal Name) que fazem parte de grupos privilegiados;

2.308. Validação de contas anormais nos grupos administrativos padrão do AD;

2.309. Validação de consistência no container adminSDHolder;

2.310. Validação de delegação Kerberos perigosa;

2.311. Validação em permissões de objetos raiz que permitem ataques do tipo DCSync;

2.312. Validação de políticas de senha fracas aplicadas aos usuários; 2.313. Validação das permissões relacionadas às contas do Azure AD Connect;

2.314. Validação do ID do grupo primário do usuário (Primary Group ID);

2.315. Validação de permissões em GPOs sensíveis associadas aos Containers Configuration, Sites, Root Partition e OUs sensíveis como Domain Controllers;

2.316. Controladores de domínio gerenciados por usuários ilegítimos;

2.317. Validação de certificado mapeado através de atributo altSecurityIdentities em contas privilegiadas;

2.318. Validação de uso de protocolo Netlogon inseguro (Zerologon/CVE-2020-1472);

2.319. A solução deve identificar vulnerabilidades e configurações incorretas do AD à medida que são introduzidas sendo:

2.320. Identificar todas as vulnerabilidades e configurações incorretas no AD;

2.321. Monitorar relações de confiança perigosas em toda a estrutura AD;

2.322. Apresentar ameaças e alterações sem a necessidade de scans estáticos e programados no Active Directory e sua infraestrutura;

2.323. Apresentar as ameaças e alterações em tempo real ou em menos de cinco minutos;

2.324. DETECÇÃO DE ATAQUES AO AD EM TEMPO REAL:

2.325. Monitorar continuamente os indicadores de possíveis ataque como DCSync, DCShadow, Password Spraying, Password Guessing/Brute Force, Lsaas Injecton nos controladores de domínio, Golden Ticket, NTLM Relay, entre outros;

2.326. Detecção de ataques ao AD em tempo real ou em menos de um minuto;

2.327. Análise detalhada do ataque, apresentando ativo de origem, vetor de ataque, controlador de domínio afetado, técnica aplicada;

2.328. Apresentação de ataques em uma linha do tempo;

2.329. Investigar ameaças, reproduzir ataques e procurar por backdoors;

2.330. Permitir busca ágil de eventos específicos na base da solução através de queries customizadas;

2.331. A solução deve ser capaz de enviar alertas por e-mail;

2.332. A solução nativamente deve ser capaz de se integrar com SIEM através de protocolo SYSLOG;

2.333. A solução deve ser capaz de filtrar e enriquecer os eventos que serão enviados para o SIEM;

2.334. A solução deve produzir regras YARA na detecção de ataques (Ex. DCSync, Golden Ticket) identificados pela ferramenta;

2.335. A solução deve possuir conjunto de APIs REST, todas as chamadas disponíveis devem estar contidas na documentação;

2.336. A solução deve permitir a criação de listas de exclusões, suportando minimamente Exclusão por domínios do AD monitorados e por itens analisados;

2.337. A solução deve ser licenciada pelo número de usuários habilitados;

2.338. DO GERENCIAMENTO DA SUPERFÍCIE DE ATAQUE

2.339. Deve avaliar a superfície de ataque externo, apresentando como a organização e seus ativos expostos na Internet são vistos pelos atacantes e quais as vulnerabilidades encontradas.

2.340. Deve identificar ativos usando registros DNS, endereços IP e ASN.

2.341. Deve possuir mecanismo de busca personalizada em base em filtros customizados.

2.342. Deve permitir exportação de dados nos seguintes padrões:

2.343. CSV

2.344. JSON

2.345. XLSX

2.346. Deve avaliar a postura de segurança de toda a sua superfície de ataque externo incluindo entradas de filtro do tipo:

2.347. Screenshot da aplicação web.

2.348. Tags personalizadas
2.349. Networking

2.350. IP

2.351. ASN 2.352. CDN

2.353. SaaS

2.354. PaaS

2.355. IaaS

2.356. Remote Access

2.357. Host

2.358. Domain

2.359. Proxy Reverso

2.360. Tipo de serviços

2.361. SSL/TLS

2.362. SSL / TLS Expiration

2.363. SSL / TLS Fingerprint

2.364. SSL / TLS Cypher Suites

2.365. SSL / TLS protocol

2.366. SSL / TLS error

2.367. SSL / TLS Serial Number

2.368. Cookie compliance

2.369. RBL

2.370. Localização

2.371. País

2.372. Cidade

2.373. Latitude

2.374. Longitude

2.375. Time Zone

2.376. Web applications

2.377. Redes Sociais
2.378. HTTP response

2.379. HTTP headers

2.380. HTTP Security headers

2.381. Whois

2.382. Estrutura de Marketing como:

2.383. Google Analytics

2.384. Google Adsense

2.385. CRM 2

.386. SEO

2.387. Media

2.388. Webcams

2.389. Printers

2.390. Video Players

2.391. Media Servers

2.392. Deve sugerir domínios a serem analisados com base nas entradas de registro inicialmente analisados.

2.393. Deve possuir integração com ServiceNow e Slack para notificações automáticas.

2.394. Deve possuir um dashboard com interação gráfica via web, para acompanhamento das vulnerabilidades encontradas.

3. Item 3 – Serviço Gerenciados de visibilidade, conformidade, segurança e orquestração dos dispositivos conectados à rede corporativa por 36 meses.

3.1. Características Gerais

3.2. A solução deverá ser fornecida e formato de appliances virtuais;

3.3. O fornecimento deve contemplar solução gerenciamento central de múltiplos appliances virtuais, bem como integração com soluções de terceiros a partir de protocolos abertos, tais como SQL, LDAP e Web Services;

3.4. As licenças poderão ser distribuídas em múltiplos appliances virtuais, gerenciados centralmente, em unidades de 1000 licenças, conforme a necessidade do **CONTRATANTE**;

3.5. Não poderá haver limitação no número de appliances virtuais gerenciados;

3.6. A solução deverá ser fornecida em formato de appliance virtual compatível com o VMware ESXi, Microsoft
HyperV e Linux KVM, podendo ser utilizados on-premises e, também, em nuvem pública AWS e Azure;

3.7. Deve monitorar todo o tráfego da rede através de uma porta espelhada no switch core (porta SPAN);

3.8. Deve realizar todas as suas funções sem a utilização de agentes (AGENTLESS) instalados nas máquinas corporativas (estações de trabalho, servidores, dentre outros);

3.9. Deve criar e manter atualizada, em tempo real, a lista de todos os elementos da rede, incluindo equipamentos de rede, impressoras, dispositivos de usuários finais, servidores, sistemas operacionais, aplicações, processos, portas abertas, dispositivos periféricos, vulnerabilidades e usuários, permitindo o agrupamento automático baseado em condições, e a aplicação automática de ações de controle de acesso, garantia de conformidade (remediação) e orquestração de segurança;

3.10. Deve ser capaz de classificar automaticamente impressoras, dispositivos de rede, máquinas Windows,
Linux e Macintosh, Dispositivos Móveis e dispositivos que estejam realizando tradução de endereços (NAT);

3.11. Deve ser capaz de diferenciar máquinas corporativas de máquinas não corporativas;

3.12. Deve ser capaz de classificar os dispositivos de IT (Information Technology) e OT (Operational Technology) por função em subcategorias, no mínimo:

3.13. IT: Computador, Mobile, Networking, Storage, Acessórios (ex: impressoras);

3.14. OT: Sistema de Aquisição de Dados, Monitoramento Ambiental, Sistema de Controle Industrial, Segurança Física (ex: Cameras IP), Monitoramento e Controle Remoto,

Saúde.

3.15. Deve ser capaz de classificar dispositivos por sistema operacional contendo, no mínimo as seguintes categorias: Alcatel-Lucent, Android, Avaya, Chrome OS, Cisco IOS, Cisco ASA-OS, Cisco Access Points, ExtremeXOS, FortiOS, Huawei VRP, iOS, LG Web OS, Linux, Macintosh, UNIX, Windows;

3.16. Deve ser capaz de classificar dispositivos por fabricante e modelo para dispositivos IoT (Internet of Things), tais como wearables e dispositivos móveis, e OT (Operational Technology), tais como sistemas de controle industrial;

3.17. Deve ser capaz de realizar a classificação passiva de dispositivos para que a classificação seja realizada sem contato ativo direto com o dispositivo (ex: para dispositivos que controlam processos operacionais de tempo real);

3.18. Deve ser capaz de criar inventário das informações da rede e dos dispositivos catalogando, pelo menos, sistemas operacionais e respectivas versões, máquinas e respectivas versões dos sistemas operacionais Windows, Linux e Mac, processos em execução (Windows, Linux e Mac), portas de comunicação abertas nos dispositivos, aplicações instaladas em Windows, dispositivos externos conectados, usuários registrados como visitantes, dentre outras;

3.19. Deve permitir o controle de acesso à rede baseado em perfis e regras de conformidade;

3.20. Deve prover funções de visibilidade e controle para ambientes de nuvem nas seguintes plataformas: AWS,
Azure, VMWare vCenter, VMWare NSX e VMWare vSphere;

3.21. Deve possuir autenticação de usuários com LDAP, RADIUS, Active Directory e 802.1x, possuindo, ainda, um servidor RADIUS e RADIUS Proxy integrado para facilitar o deployment baseado em 802.1x;

3.22. Deve suportar segurança 802.1x pre-connect e controle 802.1x post-connect tanto para rede cabeada como rede sem fio tanto de usuários corporativos como visitantes;

3.23. Deve suportar RADIUS authentication, authorization e accounting;

3.24. Deve possuir catálogo de MAC Addresses para suportar Mac Address Bypass para dispositivos que não suportam 802.1x;
3.25. Deve permitir que a autenticação 802.1x seja realizada através de servidor Microsoft Active Directory e servidor RADIUS externo (RADIUS Proxy);

3.26. Deve ser capaz de atribuir labels aos dispositivos baseados em listas de MAC Addresses mantidos em servidores FTP ou LDAP;

3.27. Deve permitir a automação do registro de convidados, tanto na rede cabeada como na rede sem fio, através de captive portal, sem necessidade de configuração/reconfiguração de equipamentos de acesso (switches);

3.28. Deve identificar automaticamente os servidores de DNS da rede;

3.29. Deve garantir a conformidade das configurações das máquinas corporativas (estações de trabalho, servidores, dispositivos móveis, dentre outros) com as políticas de segurança da organização, incluindo controle das soluções baseadas em agentes, tais como antivírus, patches de sistema operacional e bloqueio de software não-autorizado;

3.30. Deve realizar a detecção de ameaças baseada em análise do comportamento dos dispositivos (pósadmissão) não baseada em assinaturas (ex: Port Scan (TCP/UDP), Ping Sweep Scan, SNMP Scan, User Scan, Tentativa de Infecção via rede) e permitir o monitoramento e bloqueio do dispositivo;

3.31. Deve detectar dispositivos não-autorizados, tais como switches e access points (APs), identificando ainda se é um dispositivo que realiza tradução de endereços (NAT) e se está ou não autorizado a utilizar a rede;

3.32. Deve detectar portas de switches com múltiplos hosts conectados;

3.33. Deve detectar dispositivos sem endereço IP (tais como stealthy packet capture devices projetados para furto de informações) e executar ações de bloqueio de porta do switch e mudança de VLAN;

3.34. Deve controlar os dispositivos móveis conectados à rede em tempo real;

3.35. Deve possuir inventário e controle da rede em tempo real, permitindo rastrear e controlar usuários, aplicações, processos, portas e dispositivos externos;

3.36. Deve ser capaz de definir segmentos de rede baseados em endereços IP e filtrar os dados apresentados baseados em segmentos;

3.37. Deve permitir a criação de subsegmentos para diferenciar os setores e poder aplicar as políticas em diferentes segmentos;

3.38. Deve ser capaz de definir unidades organizacionais baseadas em segmentos de rede e filtrar os dados baseados em unidades organizacionais;

3.39. Deve ser capaz de realizar avaliação de postura de segurança de dispositivos IoT (Internet of Things) através da avaliação do uso de credenciais (SNMP, SSH e Telnet):

3.40. Padrão/Default de fábrica;

3.41. Base do fabricante de credenciais fracas/comuns;

3.42. Credenciais fornecidas manualmente pelo administrador.

3.43. Deve possuir módulo de relatórios e dashboard para monitoramento do nível de conformidade (compliance);

3.44. Deve possuir mecanismo para scanear máquinas Windows em busca de IOC's (Indicators of Compromise) e executar ações em resposta à identificação de máquinas comprometidas;

3.45. Cada IoC deverá poder ser composto, pelo menos, dos seguintes atributos: Nome da Ameaça, Nome do Arquivo, Tamanho do Arquivo, Hash do Arquivo, Tipo de Função Hash Utilizada, Severidade, Endereço de Central de Comando & Controle (CnC);

3.46. Deve possuir mecanismo automático de remoção de IoC's da base de dados da solução de acordo com a severidade e tempo de existência do IoC;

3.47. Deve permitir a automação e orquestração de soluções de terceiros a partir de eventos detectados pela solução, utilizando-se das capacidades de integração em ações definidas nas políticas da solução;

3.48. As ações devem poder ser encadeadas através de agendamento da sua execução permitindo a orquestração de resposta a incidentes através de comunicação com soluções de terceiros via protocolos abertos (LDAP, SQL e Web Services);

3.49. Deve ser capaz de detectar novos dispositivos de rede a partir de traps SNMP v1, v2c e v3 enviados pelos switches;

3.50. Deve ser capaz de executar ações e consultar informações em switches de diversos fabricantes e switches genéricos através de protocolo SNMP;

3.51. Deve suportar SNMP v1, v2c e v3 para permitir o monitoramento do appliance através de sistemas externos de monitoramento de rede;

3.52. Deve ser capaz de enviar traps SNMP para sistemas de monitoramento de rede quando ocorrerem modificações de configuração e quando os limites de utilização do sistema forem ultrapassados (ex: número de dispositivos gerenciados, utilização de CPU, utilização de memória, perda de pacotes etc.);

3.53. Deve ser capaz de enviar e receber mensagens via SYSLOG;

3.54. Deve ser capaz de usar informações do tráfego DHCP para classificar os dispositivos sem a necessidade de utilização de IP Helper Address para redirecionamento das requisições DHCP;

3.55. Deve ser capaz de analisar o tráfego de rede e calcular estatísticas como tamanho médio de pacote, número médio de pacotes por segundo e resoluções de nomes via DNS;

3.56. Deve ser capaz de receber e processar informações de Flow (NetFlow v9, IPFIX e sFlow) para identificação de dispositivos e propriedades de dispositivos;

3.57. Deve ser capaz de identificar, aplicar políticas, manter a segurança e garantir a conformidade de dispositivos na nuvem pública da Amazon – AWS, inclusive identificando e controlando instâncias Elastic Compute Cloud (EC2), usuários Identity and Access Management (IAM) e Virtual Private Clouds (VPCs), permitindo:

3.58. Ver instâncias EC2, usuários IAM e VPCs;

3.59. Criar e aplicar políticas nestas entidades AWS;

3.60. Manter a segurança e conformidade das instâncias de nuvem, usuários IAM e VPCs.

3.61. Deve ser capaz de identificar, aplicar políticas, manter a segurança e garantir a conformidade de dispositivos na nuvem pública da Microsoft – Azure, inclusive identificando e controlando instâncias de Virtual Machines (VM) e Virtual Networks (VNET), permitindo:
3.62. Ver instâncias VM e redes VNETs;

3.63. Criar e aplicar políticas nestas entidades Azure;

3.64. Manter a segurança e conformidade das instâncias de VM's e VNET's.

3.65. Deve suportar a descoberta e gerenciamento de dispositivos em máquinas virtuais VMWare vSphere/vCenter;

3.66. Deve ser capaz de aplicar funcionalidades de controle em máquinas virtuais de ambientes VMWare vSphere/vCenter; 3.67. Desligar máquina virtual;

3.68. Ligar máquina virtual;

3.69. Reiniciar máquina virtual;

3.70. Colocar a máquina em espera;

3.71. Instalar e atualizar VMware Tools;

3.72. Desconectar todas as placas de redes da máquina virtual;

3.73. Alterar o Virtual Port Group da máquina virtual. 3.74. Deve ser capaz de aplicar microssegmentação em máquinas virtuais de ambientes VMWare NSX; 3.75. Deve ser capaz de identificar dispositivos e servidores configurados com o uso de credenciais comuns da empresa e que devem ser considerados inseguros;

3.76. Deve possuir trilha de auditoria acessível pela interface gráfica que registre todas as operações de modificação nas configurações da solução (adições, edições e remoções).

3.77. ATRIBUTOS E PROPRIEDADES

3.78. Deve ser capaz de identificar atributos e propriedades dos dispositivos para permitir a criação de políticas baseadas em condições, no mínimo:

3.79. Autenticação: Identificar autenticação via HTTP (80/TCP), Telnet(23/TCP), NetBIOS(139/TCP), FTP(21/TCP)
IMAP (143/TCP), POP3(110/TCP), rlogin(513/TCP) e Active Directory;

3.80. Dispositivo: banners de serviço, endereço IP, nome DNS, se está realizando NAT, usuário logado, interfaces de rede, resultados de scripts, portas abertas, número de endereços IPv4 e IPv6, NIC Vendor, NetBIOS Hostname, NetBIOS Domain, qualquer atributo SNMP do dispositivo, resultado de comando via SSH;

3.81. Usuário: nome, status da autenticação e grupo de trabalho;

3.82. Windows Active Directory: conta desabilitada, conta expirada, Display Name, Member Of, Email, Initials,
etc;

3.83. Sistema Operacional (Windows/Linux/Mac): tipo e versão do SO; processos em execução; existência, data e tamanho de arquivos; resultado de execução de scripts, usuário logado;

3.84. Detalhes de Máquinas Windows: domínio, último evento de login, existência e valores de chaves de registro, serviços instalados, serviços em execução, vulnerabilidades, dispositivos externos;

3.85. Detalhes de máquinas virtuais: Health Status de máquinas Guest VMWARE e tipo de instância Amazon EC2;

3.86. Segurança: agente de antivírus instalado, nível de atualização e status de firewall, IoC's (Indicators of Compromise), ARP Spoofing, sessões abertas como cliente,

sessões abertas como servidor, traps SNMP recebidas da porta onde o dispositivo está conectado;

3.87. Aplicações Windows: aplicações instaladas, incluindo versão, aplicações de Cloud Storage, Instant Messaging, Criptografia de Disco e Peer to Peer instaladas e em execução;

3.88. Periféricos: tipo do dispositivo, fabricante e tipo de conexão;

3.89. Rede: segmento de rede, switch e porta ao qual o dispositivo está conectado, VLAN.

3.90. Deve ser capaz de criar novas propriedades/atributos para os dispositivos usando o resultado de scripts executados nos dispositivos (ex: quantidade de instâncias de um determinado processo em execução em servidores Linux);

3.91. Deve ser capaz de criar novas propriedades/atributos para os dispositivos baseado em valores consultados em bases de dados externas via SQL, Web Services e LDAP;

3.92. Deve ser capaz de criar novas propriedades baseado na comparação entre propriedades já existentes;

3.93. Deve ser possível criar listas de valores de propriedades para serem usadas como operandos em regras de políticas (Ex: Listas de Endereços IP, Listas de Nomes de Máquinas, Listas de Processos, etc);

3.94. Deve ser possível detectar mudanças de valores em propriedades tais como: aplicações Windows instaladas e/ou removidas, novas interfaces de rede, mudança de data, tamanho e versão de arquivos Windows, criação/remoção de arquivos Windows, mudança de endereço IP, mudança de nome no DNS, alterações no Windows Registry, mudança de porta no switch, dentre outras, e utilizá-las como condições nas regras das políticas para execução de ações;

3.95. Deve ser possível utilizar atributos e propriedades para organizar os dispositivos em grupos, de forma a permitir melhor controle sobre a aplicação de políticas.

3.96. AÇÕES

3.97. Deve ser possível definir os seguintes tipos de ações automáticas nas políticas:

3.98. Restringir o acesso através de modificação de VLAN, desabilitar porta de switch e TCP Resets (Firewall Virtual);

3.99. As ações de Firewall Virtual (TCP Resets) devem poder ser realizadas no tráfego originado pelo dispositivo e no tráfego destinado ao dispositivo; 3.100. Bloquear acesso de e para hosts e portas específicas;

3.101. Deve ser possível especificar o segmento de rede/faixa de IP e portas que estão impedidos de se comunicar com o dispositivo bloqueado;

3.102. Deve ser possível criar exceções à regra para permitir o acesso de administradores ao dispositivo;

3.103. A solução deve realizar ação de Virtual Firewall sem modificação na infraestrutura utilizando, apenas, informações coletadas no espelhamento de porta (Port SPAN).

3.104. Notificar o usuário através de redirecionamento de tráfego HTTP a partir da escuta do tráfego espelhado (SPAN port), inclusive em ambientes que utilizam Web Proxy;

3.105. Deve ser possível redirecionar o tráfego para qualquer URL definida pelo administrador;

3.106. Deve ser possível criar exceções para impedir o redirecionamento de tráfego direcionado a URL’s específicas;

3.107. Deve ser possível criar exceções para impedir o redirecionamento de tráfego para segmentos de rede e faixas de IP específicas;

3.108. A solução deve realizar ação de redirecionamento de tráfego HTTP sem modificação na infraestrutura utilizando, apenas, informações coletadas no espelhamento de porta (Port SPAN).

3.109. Redirecionar tráfego usando HTTPS;

3.110. Bloquear tráfego HTTPS passando através de servidor Proxy;

3.111. Permitir redirecionar os usuários para páginas de autenticação e de ações de remediação;

3.112. A solução deve realizar ação de redirecionar os usuários para página de autenticação sem modificação na infraestrutura utilizando, apenas, informações coletadas no espelhamento de porta (Port SPAN)

3.113. Permitir definir exceções para URL’s específicas;

3.114. Registrar convidados através de formulário de registro (captive portal) para máquinas não corporativas (terceiros, visitantes, BYOD), tanto para acessos via rede cabeada como rede sem fio, sem necessidade de configuração/reconfiguração de equipamentos de acesso (ex: switches), com as seguintes capacidades:

3.115. Permitir definir a validade de tempo de acesso do usuário;

3.116. Capacidade de definir diversos tipos de convidados com privilégios diferenciados;

3.117. Atribuir limitações de rede de acordo com o usuário;

3.118. Formulário de auto registro com acesso automático, sem necessidade de aprovação;

3.119. Formulário de auto registro com envio de códigos de verificação via e-mail para permitir o acesso (one time password);

3.120. Formulário de auto registro com aprovação de acesso por “sponsor” devidamente autorizado

3.121. Controlar o acesso do convidado até que o seu acesso seja aprovado pelo “sponsor” indicado;

3.122. Possuir Dissovable Agent para levantamento de informações e aplicação de políticas de conformidade em máquinas não corporativas, sem necessidade de permissões de administrador para execução e sem processo de instalação, não deixando nenhum rastro após o reboot.

3.123. Redirecionamento de tráfego via DNS (DNS Enforcement);

3.124. Comunicação: enviar e-mail de alertas aos usuários e administradores, notificar de usuário através de redirecionamento HTTP, enviar traps SNMP, envio de registros para SYSLOG;

3.125. Remediação de sistema operacional Windows: instalar patch de sistema operacional; criar e modificar chaves de registro; iniciar agente de segurança e atualizar assinaturas; desabilitar dispositivo externo, encerrar processos de Cloud Storage, P2P e IM;

3.126. Iniciar e encerrar processos e scripts em Windows, Linux e Mac;

3.127. Executar scripts no dispositivo com passagem de parâmetros para o script com valores dos atributos disponíveis sobre o dispositivo;

3.128. Deve ser possível executar scripts como “root” em dispositivos Linux usando “sudo”.

3.129. Executar scripts no servidor da solução com passagem de parâmetros para o script com valores de atributos disponíveis do dispositivo;

3.130. Bloquear tráfego malicioso e colocar em quarentena dispositivo malicioso;

3.131. Atribuir dispositivos a grupos para utilização como critério de filtragem em políticas;

3.132. Enviar comandos para soluções de terceiros, através de protocolo aberto (SQL, LDAP e Web Services);

3.133. Iniciar atualizações de segurança do Windows, via Microsoft Web site ou WSUS;

3.134. Deve permitir escolher um dos três métodos de atualização disponíveis na plataforma: download e instalação automáticas, download automático e notificação do usuário, usando as configurações de “automatic update” do dispositivo.

3.135. A solução deve ser fornecida com plugin específico de integração com a solução de gestão de vulnerabilidades ofertada pela CONTRATADA;

3.136. Deve possuir um assistente, via WEB, que permita aos próprios usuários aplicarem ações de remediação de vulnerabilidades do sistema operacional Windows que tenham sido detectadas no dispositivo;

3.137. Todas as ações executadas sobre um dispositivo devem ser registradas (log) nas informações detalhadas do dispositivo.

3.138. POLÍTICAS

3.139. As políticas devem ser compostas por regras de condição e execução de ações em um escopo específico;

3.140. Deve permitir a limitação de escopo de aplicação da política baseado em faixas de endereço IP, segmentos de rede e grupos de dispositivos;

3.141. Deve permitir criar exceções para escopo de políticas baseado em endereço IP, MAC Address, NetBIOS Hostname; Username e grupos de dispositivos;

3.142. As regras de cada política devem ser criadas com base em condições lógicas (AND, OR, NOT) sobre quaisquer propriedades/atributos e informações levantadas sobre cada dispositivo;

3.143. Deve ser possível definir se o resultado da avaliação de uma condição será verdadeiro ou falso em caso de ausência de informações sobre a propriedade/atributo que está sendo avaliado;

3.144. Cada regra deve suportar a execução de múltiplas ações e o agendamento das mesmas para permitir flexibilidade na implementação de ações de controle de acesso, remediação e orquestração de segurança;

3.145. O agendamento de ações deve suportar pelo menos as seguintes opções:

3.146. Imediatamente;

3.147. Após um intervalo de tempo definido pelo administrador;

3.148. Data e hora específica. 3.149. Deve ser possível estabelecer a duração da aplicação das ações com as seguintes opções:

3.150. Sem data final;

3.151. Após um intervalo de tempo definido pelo administrador;

3.152. Data e hora específica.

3.153. Deve ser possível atribuir labels aos dispositivos e criar contadores para implementar lógicas de políticas complexas, capazes de reter o estado do dispositivo durante os processos de reverificação das condições lógicas;

3.154. Deve permitir a criação de um catálogo de condições customizadas para serem reutilizadas em regras de diferentes políticas;

3.155. Deve ser possível definir novas propriedades do dispositivo baseado na comparação ente outras propriedades já existentes;

3.156. As políticas criadas pelo administrador deverão permitir estabelecer condições de classificação e conformidade (compliance) de dispositivos, bem como definir ações automáticas de remediação, tais como:

3.157. Identificar hosts e colocar em quarentena quando não houver o software de antivírus instalado ou não estiver com os patches de sistema atualizados;

3.158. Limitar acesso à rede para convidados;

3.159. Ativar detecção automática para hosts que estão faltando service pack e integrar com ferramenta de correção (WSUS);

3.160. Verificar todos os servidores que não estão em conformidade (compliance) com as políticas;

3.161. Automaticamente deverá descobrir e colocar em quarentena os access points (APs) wireless desconhecidos.

3.162. Deve possuir capacidade de atualizar bases de dados externas via comandos SQL parametrizados com dados dos dispositivos disponíveis na solução;

3.163. Deve ser capaz de executar comandos em soluções de terceiros através de chamadas de Web Services parametrizados com dados dos dispositivos disponíveis na solução;

3.164. Deve possuir capacidade de buscar informações em soluções de terceiros, através de LDAP, SQL e Web
Services, para aplicação de políticas de segurança, controle de acesso e conformidade de dispositivos;

3.165. Deve possibilitar a importação e exportação de políticas;

3.166. Deve fornecer as informações sobre os dispositivos em tempo real;

3.167. Deve possuir templates de políticas pré-definidas e assistente gráfico para permitir a criação rápida de políticas padrão;

3.168. Deve permitir detectar usuários e dispositivos que estão fora de conformidade com a política de segurança, informando na console a razão da não-conformidade e detalhes completos do usuário/dispositivo, permitindo ainda a aplicação de ações automáticas de remediação;

3.169. Deve executar envio de alertas, restrições de acesso e ações de remediação automáticas, incluindo:
3.170. Atribuição de um dispositivo a VLANs específicas para controle de acesso;

3.171. Migração do dispositivo automaticamente para rede de convidados;

3.172. Migração de um dispositivo da rede de produção para uma rede de quarentena;

3.173. Finalização de aplicações não-autorizadas nas estações de trabalho e servidores corporativos.

3.174. INVENTÁRIO EM TEMPO REAL

3.175. Deve possuir inventário de usuários, dispositivos, software, hardware e rede com, no mínimo, as seguintes categorias:

3.176. Inventário de usuários da rede;

3.177. Inventário de convidados registrados incluindo status da aprovação de acesso, identificação do aprovador e da pessoa de contato indicada durante o processo de registro;

3.178. Inventário de portas de comunicação abertas associadas aos respectivos dispositivos;

3.179. Inventário de vulnerabilidades Microsoft associadas aos respectivos dispositivos;

3.180. Inventário de hardware de máquinas Windows contendo:

3.181. Informações gerais do equipamento: número de processadores, total de memória física, fabricante, modelo, time zone;

3.182. Discos: tipo do drive, nome do volume, tamanho, espaço disponível;

3.183. Monitores: tipo e fabricante; 3.184. Placa mãe: fabricante e modelo;

3.185. Adaptadores de rede: índice, endereço MAC, endereço IP, subrede IP e default gateway;

3.186. Memória física: capacidade, tipo, velocidade e fabricante;

3.187. Dispositivos Plug-and-Play: Class GUID, Device ID e fabricante;

3.188. Processador: fabricante, arquitetura, família, max clock speed, número de cores, percentual de carga e status.

3.189. Inventário de dispositivos externos conectados em máquinas Windows (wireless, impressoras, adaptadores de rede, modems, dispositivos de imagem, drives de disco externo, DVD/CDROM, bluetooth);

3.190. Inventário de aplicações instaladas em ambientes Windows e Mac;

3.191. Inventário de switches com informação de número de dispositivos conectados por porta.

3.192. Deve permitir integrar-se com bases de dados e soluções externas para atualização imediata de informações de inventário de dispositivos existentes e de novos dispositivos que se conectarem à rede usando SQL e Web Services;

3.193. Deve permitir a criação de listas baseadas no inventário, tais como listas de aplicações autorizadas e nãoautorizadas.

3.194. CONSOLE DE GERENCIAMENTO
3.195. Toda informação detectada deverá ser unificada em uma única console de gerenciamento central oferecida pelo próprio fabricante capaz de gerenciar múltiplos appliances;

3.196. A Console de Gerenciamento Central deve ser capaz de atribuir a cada appliance o conjunto de segmentos de rede a ser monitorado/controlado por cada um;

3.197. Deverá possuir painéis/telas que apresentem:

3.198. Políticas, regras e detalhes dos dispositivos que caíram no escopo e nas regras estabelecidas com capacidade de filtragem por segmento, unidade organizacional e grupos e mecanismo de busca baseado em texto;

3.199. A tela/painel deverá mostrar tabela customizável com detalhes dos dispositivos, como:

3.200. Endereço Mac; 3.201. Endereço IP;

3.202. Segmento de rede;

3.203. Nome DNS e NetBIOS; 3.204. Switch, porta e VLAN de conexão do dispositivo;

3.205. Nome/Login do usuário;

3.206. Ações executadas sobre o dispositivo. 3.207. Deve ser possível customizar as propriedades dos dispositivos a serem apresentados na tabela; 3.208. Para cada máquina selecionada na tela/painel deverá ser possível:

3.209. Visualizar as políticas e regras em que o dispositivo foi enquadrado, informando data e hora, e as políticas e regras em que o dispositivo não foi enquadrado informando a razão de o mesmo não ter sido avaliado;

3.210. Exibir todos os detalhes (atributos e propriedades) do dispositivo selecionado;

3.211. Informações de compliance do dispositivo selecionado:

3.212. Inventário de usuários, dispositivos, aplicações e informações de rede com capacidade de filtragem por segmento, unidade organizacional e grupos e mecanismo de busca baseado em texto;

3.213. Criação, modificação e configuração de políticas;

3.214. Ameaças detectadas com capacidade de filtragem por segmento, unidade organizacional e grupos e mecanismo de busca baseado em texto.

3.215. Deve possuir assistente web de customização de aparência das telas de notificação e login via HTTP e do portal de gerenciamento de convidados;

3.216. Deve permitir que aplicações de terceiros consultem e atualizem propriedades/atributos dos dispositivos através de chamadas de Web Services disponíveis na solução.

3.217. Deve possuir portal WEB para consulta rápida de todos os detalhes dos dispositivos com facilidade de busca baseada em atributos do dispositivo, no mínimo por endereço IPv4, endereço IPv6, login do usuário, nome DNS, IP do switch onde o dispositivo está conectado, NetBios Domain, NetBios Hostname, e VMWare ESXi Server Name;

3.218. Deve permitir a visualização de registro de auditoria, contendo informações sobre as atividades dos administradores da solução em um período de tempo específico;

3.219. Deve permitir a visualização de log de eventos detectados pelas políticas da solução, atualizado em tempo real e filtrado por faixa de endereços IP e período de tempo, para permitir a investigação das atividades de dispositivos específicos;

3.220. Deve permitir a visualização dos logs de sistema (system logs) e envio dos mesmos para um servidor Syslog externo;

3.221. Deve fornecer opção de remediação, restrição de acesso e comunicação com o usuário final diretamente a partir da console, no mínimo:

3.222. Criar exceções para dispositivo;

3.223. Reverificar status do dispositivo;

3.224. Bloquear ou colocar em quarentena máquina em uma VLAN;

3.225. Bloquear acesso à internet;

3.226. Finalizar um processo;

3.227. Forçar autenticação na rede;

3.228. Possibilitar realizar a reverificação do dispositivo, por demanda, para todas as políticas ou apenas as selecionadas;

3.229. Possibilitar filtrar dispositivos baseado em segmentos de rede, unidades organizacionais e grupos;

3.230. Possibilitar visualizar apenas os dispositivos submetidos à classificação passiva;

3.231. Deve possuir mecanismos de limitação (threshold) de aplicação de ações de bloqueio e limitação de acesso baseado em percentual do número de dispositivos controlados, incluindo, pelo menos, as ações de desabilitar porta de switch, modificação de VLAN, TCP Reset (Firewall Virtual), notificação via HTTP, redirecionamento via HTTP e matar processos em máquinas Windows.

3.232. RELATÓRIOS E DASHBOARD

3.233. Deve possuir facilidade para geração e agendamento de relatórios com informações de tempo real sobre políticas, compliance de dispositivos, vulnerabilidades de máquinas Windows, informações do inventário, detalhes de dispositivos, ativos de rede e usuários visitantes; 4.

3.234. Deve possuir relatório/gráfico de tendência de políticas ao longo do tempo para permitir a avaliação da evolução de questões de classificação e compliance de dispositivos;

3.235. Todos os relatórios devem poder ser filtrados, pelo menos, por segmento de rede;

3.236. Todos os relatórios devem permitir agendamento e envio por e-mail;

3.237. Os relatórios que apresentem detalhes dos dispositivos devem permitir ao administrador selecionar, dentre todos os atributos dos dispositivos, aqueles que devem ser apresentados no relatório;

3.238. Deve possuir dashboard customizável que apresente de forma gráfica e dinâmica informações de classificação, conformidade e estado de gerenciamento dos dispositivos;

3.239. O dashboard deve ser composto por Widgets customizáveis que apresentem gráficos com dados
estatísticos coletados das políticas e regras de classificação/compliance criadas pelo administrador;
3.240. Os Widgets devem permitir modificar dinamicamente o período de tempo apresentado no gráfico;

3.241. Os Widgets que apresentem gráficos de tendência de regras de compliance devem possuir setas indicativas de tendências de melhoria ou piora nos seus níveis:

3.242. Deve ser possível customizar o sentido das setas indicativas para indicar qual das direções (cima/baixo) indica melhoria do nível de compliance;

4. SERVIÇOS GERENCIADOS COM MONITORAMENTO E RESPOSTA A OCORRÊNCIAS APLICÁVEL AOS ITENS 1, 2, 3 e 4

4.1. Características do Serviço

4.2. A **CONTRATADA** será responsável por projetar, instalar, configurar, gerenciar e monitorar a solução ofertada;

4.3. A **CONTRATADA** deverá elaborar um projeto de implantação contendo gerenciamento de escopo, risco, mudanças, cronograma de instalação, gerenciamento de recursos humanos, contendo planejamento detalhado para permitir uma instalação com o menor risco de impacto possível, detalhando o passo a passo dos serviços;

4.4. A **CONTRATADA** deverá cumprir com todas as exigências técnicas e funcionais relacionadas com a solução ofertada, que devem ser implantadas durante o período contratado, sem ônus para o **CONTRATANTE**;

4.5. O fornecimento de toda e qualquer ferramenta, instrumento, material e equipamento de proteção, bem como materiais complementares estritamente necessários à instalação ou à assistência técnica é de inteira responsabilidade da **CONTRATADA** e não deverá gerar ônus ao **CONTRATANTE**;

4.6. No processo de instalação o Responsável Técnico deverá tomar todas as medidas necessárias visando garantir a perfeita execução do serviço (instalação e configuração);

4.7. No prazo de até 10 (dez) dias após a conclusão de instalação da solução ofertada, a contratada deverá fornecer documentação final contendo as configurações e topologias de como foi instalada a solução;

4.8. A documentação deverá ser aprovada pelo **CONTRATANTE** e pelo Gestor Técnico do **CONTRATANTE**, caracterizando a homologação da solução em um prazo de 5 dias, quando o **CONTRATANTE** emitirá um Termo de Aceite Definitivo (TAD);

4.9. Caso seja identificado defeito ou falha sistemática em determinado produto/serviço entregue pela **CONTRATADA**, ou ainda, que nos testes realizados sejam considerados em desacordo com as especificações técnicas requeridas, a o Gestor Técnico do **CONTRATANTE** pode exigir a substituição, total ou parcial, do referido produto;

4.10. A **CONTRATADA** será responsável pelo monitoramento da solução em regime 24x7, devendo manter a mesma sempre atualizada e em operação;

4.11. O monitoramento deverá ser realizado através de ferramentas próprias da **CONTRATADA** integradas via API com a console/servidor de gerenciamento central para automação de coleta de alertas críticos e acionamento imediato da equipe da **CONTRATADA**;

4.12. A ocorrência de alertas de alta criticidade devem acionar diretamente, de forma automática, através de alarme sonoro em aplicativo de celular, os técnicos de plantão da **CONTRATADA** para início imediato do tratamento da ocorrência, dentro dos prazos definidos no ANS, sendo reportados imediatamente ao preposto do **CONTRATANTE** para ciência do fato;
4.13. A **CONTRATADA** deverá informar mensalmente a escala de técnicos de sobreaviso que atenderão os alertas de alta criticidade durante o período do plantão;
4.14. À opção do **CONTRATANTE**, esta poderá indicar até 5 profissionais para receberem os alarmes em tempo real, de forma simultânea, no aplicativo de celular a ser fornecido pela **CONTRATADA** sem custos adicionais.

4.15. O tratamento das ocorrências geradas pelo sistema de monitoramento automático deve ser acompanhado através de plataforma de gestão automatizada de processos (BPMn) fornecido pela **CONTRATADA**, que indique claramente e controle os prazos para execução de cada etapa do processo de resposta aos incidentes detectados;

4.16. O processo de tratamento de incidentes deve conter pelo menos as seguintes características:

4.17. Notificação imediata da **CONTRATADA** sobre a ocorrência detectada;

4.18. Investigação da ocorrência através dos recursos fornecidos pela solução;

4.19. Determinação da real criticidade da ocorrência;

4.20. Execução de ações de contenção previamente acordadas com o cliente;

4.21. O processo automatizado deve ser capaz de tratar de forma diferenciada pelo menos 4 níveis de criticidade de alertas;

4.22. O processo automatizado deve ser capaz de enviar e-mail e alertas em aplicativo de celular de forma automática para a **CONTRATADA** e para o **CONTRATANTE**;

4.23. O processo automatizado deve ser capaz de emitir avisos sonoros através de aplicativo de celular para os técnicos da **CONTRATADA** e do **CONTRATANTE**, com diferentes graus de intensidade a depender do nível de criticidade da situação detectada;

4.24. Deve permitir a customização, para cada **CONTRATANTE**, de quais tipos de alertas se enquadram em cada um dos níveis de criticidade.

4.25. Deve ser disponibilizado para o **CONTRATANTE** um dashboard de acompanhamento em tempo real dos processos de tratamento dos incidentes que apresente, no mínimo:

4.25.1. Tarefas em aberto com indicação do responsável pela sua execução e tempo restante para finalização da mesma de acordo com o ANS contratado;

4.25.2. Tarefas em atraso com indicação do responsável pela sua execução e tempo de atraso em relação ao ANS contratado;

4.25.3. Tabela de atraso médio de tarefas já encerradas;

4.25.4. Tabela de tempo médio de execução de tarefas já encerradas.

4.26. A manutenção visa manter em perfeito estado de operação os serviços fornecidos em atendimento ao objeto, deste modo a **CONTRATADA** deve cumprir os seguintes procedimentos:

4.26.1. desinstalação, reconfiguração ou reinstalação decorrentes de falhas no software, atualização da versão de software, correção de defeitos, ajustes e reparos necessários, de acordo com os manuais e as normas técnicas específicas para os recursos utilizados;

4.26.2. Quanto às atualizações pertinentes aos softwares, entende-se como “atualização” o provimento de toda e qualquer evolução de software, incluindo correções,

“patches”, “fixes”, “updates”, “service packs”, novas “releases”, “versions”, “builds”, “upgrades”, englobando inclusive versões não sucessivas, nos casos em que a liberação de tais versões ocorra durante o período de garantia especificado.
4.27. Deve ser elaborado e enviado mensalmente um relatório executivo com o resumo das principais ocorrências e as providências executadas pela **CONTRATADA**, além de gráficos e estatísticas relativos à conformidade operacional do ambiente;

4.28. A operação e administração (gerenciamento total) da solução será realizada pela **CONTRATADA** conforme as orientações e solicitações de configurações e políticas realizadas pelo Gestor Técnico do **CONTRATANTE**;

4.29. As solicitações de alteração de configurações deverão ser realizadas conforme o ANS definido na Seção – Acordo de Nível de Serviço – ANS;

4.30. No caso de necessidade de ações preventivas ou corretivas o **CONTRATANTE** agendará com antecedência junto a **CONTRATADA** as implementações das correções, fora do horário comercial, preferencialmente em feriados e finais de semana. Nenhuma ação poderá ser executada sem a ciência e anuência do **CONTRATANTE**;

4.31. A **CONTRATADA** deverá prestar suporte a todos os componentes de software fornecidos para a implementação e utilização da solução;

4.32. A **CONTRATADA** deverá disponibilizar serviço de suporte técnico e manutenção, no regime (24x7) vinte e quatro horas por dia, sete dias por semana, pelo período da contratação;

4.33. Os acionamentos dos serviços de suporte e manutenção serão requisitados por meio de ordens de serviço, a serem abertas pelo **CONTRATANTE**, através de número de telefone nacional (0800 com serviço de uso ilimitado) disponibilizado pela **CONTRATADA**, e ainda, por e-mail e sítio de internet;

4.34. Não haverá limitação no número de chamados que poderão ser abertos;

4.35. A **CONTRATADA** manterá registro de todas as ordens de serviço abertas, disponibilizando, para cada uma, no mínimo as seguintes informações:

4.35.1. Número sequencial da ordem;

4.35.2. Data e hora de abertura;

4.35.3. Severidade;

4.35.4. Descrição do problema;

4.35.5. Data e hora do início do atendimento;

4.35.6. Data e hora de término do atendimento (solução).

4.36. O serviço de suporte técnico e manutenção deverá ser prestado por profissional devidamente certificado nas soluções tecnológicas utilizadas na prestação dos serviços contratados;

4.37. As informações relacionadas à ANS estão na Seção – Acordo de Nível de Serviço – ANS.

4.38. Acordo de Nível de Serviço (ANS)

4.39. A **CONTRATADA** deverá possuir Central de Atendimento (contato telefônico, sítio na Internet e e-mail) para consultas, aberturas de chamados técnicos e envio de arquivos para análise, durante 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana;

4.40. A **CONTRATADA** deverá prestar serviços de suporte técnico 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, na cidade de Salvador – BA, relativos ao objeto deste Termo de Referência, sem ônus para o **CONTRATANTE**;
4.41. A **CONTRATADA** será responsável pelo cumprimento e medição dos índices estabelecidos neste item que serão auditados pelo **CONTRATANTE** durante todo o prazo de vigência do contrato, e que poderão ser revistos, a qualquer tempo, com vistas à melhoria ou ajustes na qualidade dos serviços prestados, mediante acordo entre as partes;

4.42. Níveis de Serviço e Tempo Esperados:

4.43. Plantão Telefônico por número 0800 como serviço de uso ilimitado, no período de 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana;

4.44. No Local (on site) – Serviço de uso ilimitado, prestado em caso de emergência, ou outra necessidade maior e também compreendendo os seguintes tipos de atendimento local: suporte para upgrade de versões e releases do software; solução de problemas detectados (troubleshoot); análise e correção de eventos relacionados à segurança e à performance do software e do ambiente; atualização simultânea nos ambientes dos Órgãos e Entidades do **CONTRATANTE**.

4.45. Para efeito dos atendimentos técnicos, a **CONTRATADA** deverá observar os níveis de severidade e respectivos prazos máximos fixados abaixo:

4.46. NÍVEIS DE SEVERIDADE DOS CHAMADOS

NÍVEIS DE SEVERIDADE DOS CHAMADOS	
NÍVEL	**DESCRIÇÃO**
1	Serviços totalmente indisponíveis
2	Serviços parcialmente indisponíveis ou com degradação de tempo de resposta no acesso aos aplicativos
3	Serviços disponíveis com ocorrência de alarmes de avisos, consultas sobre problemas, dúvidas gerais sobre o equipamento fornecido

TABELA DE PRAZOS DE ATENDIMENTO AO SOFTWARE				
MODALIDADE	**PRAZOS**	**1**	**2**	**3**
On site	Início atendimento	2 horas	4 horas	24 horas
	Término atendimento	4 horas	8 horas	72 horas
Telefone, email e web	Início atendimento	2 horas	4 horas	24 horas
	Término atendimento	4 horas	8 horas	72 horas

4.47. Para o Nível 1, caso o atendimento não seja finalizado até as 20h00min, o técnico não poderá interrompêlo, devendo continuar até sua finalização, ou a interrupção do mesmo pelo **CONTRATANTE** através do Gestor do Contrato;

4.48. Após a conclusão do serviço é obrigação da **CONTRATADA** verificar o restabelecimento das condições operacionais normais;

4.49. Todo chamado somente será caracterizado como "encerrado" mediante concordância do **CONTRATANTE**;

4.50. Todo chamado de incidente, após sua solução, deverá ser finalizado com a emissão de um Relatório de Incidente a ser enviado para o **CONTRATANTE**.

4.51. Para as situações em que a solução definitiva de problemas no ambiente demande reimplantação, reestruturação ou reinstalação do produto, este deverá ser programado e planejado, com a antecedência necessária, de modo a não prejudicar a operação dos demais sistemas do **CONTRATANTE**.

APENSO II

TERMO DE COMPROMISSO DE SIGILO

O **MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA**, sediado em 5ª Avenida, n° 750, CAB - Salvador, BA - Brasil - CEP: 41.745-004, CNPJ n.º 04.142.491/0001-66, doravante denominado **CONTRATANTE**, e, de outro lado, a **CENTRO DE PESQUISAS EM INFORMÁTICA LTDA**, sediada à Av. Santos Dumont, 6216, S331 Quadra única, Loteamento Jardim Santo Antônio, Pitangueiras, Lauro de Freitas/BA, CEP 42.701-260, CNPJ n.º 40.584.096/0002-88 doravante denominada CONTRATADA;

CONSIDERANDO que, em razão do CONTRATO N.º 095/2025, a **CONTRATADA** poderá ter acesso a informações sigilosas do **CONTRATANTE**;

CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção;

CONSIDERANDO o disposto na Política de Segurança da Informação do Contratante;

Resolvem celebrar o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO, doravante TERMO, vinculado ao CONTRATO N.º 095/2025, mediante as seguintes cláusulas e condições:

Cláusula Primeira – DO OBJETO

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela Contratada, no que diz respeito ao trato de informações sigilosas, disponibilizadas pelo **CONTRATANTE**, por força dos procedimentos necessários para a execução do objeto do contrato celebrado entre as partes e em acordo com o que dispõem a Lei nº 12.527, de 18/11/2011 e os Decretos nº 7.724, de 16/05/2012 e 7.845, de 14/11/2012, que regulamentam os procedimentos para acesso e tratamento de informação classificada em qualquer grau de sigilo.

Cláusula Segunda – DOS CONCEITOS E DEFINIÇÕES

Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:

INFORMAÇÃO: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

INFORMAÇÃO SIGILOSA: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado.

Cláusula Terceira – DA INFORMAÇÃO SIGILOSA

Serão consideradas como informação sigilosa, toda e qualquer informação classificada ou não nos graus de sigilo ultrassecreto, secreto e reservado. O TERMO abrangerá toda informação escrita, verbal ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: know-how, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as atividades do **CONTRATANTE** e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não do contrato celebrado entre as partes, doravante denominados INFORMAÇÕES, a que diretamente ou pelos seus empregados, a **CONTRATADA** venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO nº 095/2025.

Cláusula Quarta – DOS LIMITES DO SIGILO

As obrigações constantes deste TERMO não serão aplicadas às INFORMAÇÕES que:

I – Sejam comprovadamente de domínio público no momento da revelação, exceto se tal fato decorrer de ato ou omissão da **CONTRATADA**;

II – Tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente TERMO;

III – Sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

Cláusula Quinta – DOS DIREITOS E OBRIGAÇÕES

As partes se comprometem a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do contrato celebrado entre as partes, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas INFORMAÇÕES, que se restringem estritamente ao cumprimento do contrato ao qual se vincula o presente termo.

Parágrafo Primeiro – A **CONTRATADA** se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento expresso e prévio do **CONTRATANTE**.

Parágrafo Segundo – A **CONTRATADA** compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do contrato ao qual se vincula o presente instrumento sobre a existência deste TERMO bem como da natureza sigilosa das informações.

I – A **CONTRATADA** deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente TERMO e dará ciência ao **CONTRATANTE** dos documentos comprobatórios.

Parágrafo Terceiro – A **CONTRATADA** obriga-se a tomar todas as medidas necessárias à proteção da informação sigilosa do **CONTRATANTE**, bem como evitar e prevenir

a revelação a terceiros, exceto se devidamente autorizado por escrito pelo **CONTRATANTE**.

Parágrafo Quarto – Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste TERMO.

I – Quando requeridas, as INFORMAÇÕES deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes.

Parágrafo Quinto - A **CONTRATADA** obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados e contratados, assim como por quaisquer outras pessoas vinculadas à Contratada, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do contrato celebrado entre as partes a qual se vincula o presente termo.

Parágrafo Sexto - A **CONTRATADA**, na forma disposta no parágrafo primeiro, acima, também se obriga a:

I. Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das INFORMAÇÕES, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;
II. Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmo judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das INFORMAÇÕES por seus agentes, representantes ou por terceiros;

III. Comunicar ao **CONTRATANTE**, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das INFORMAÇÕES, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e

IV. Identificar as pessoas que, em nome da **CONTRATADA**, terão acesso às informações sigilosas.

Cláusula Sexta – DA VIGÊNCIA

O presente TERMO tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de sua assinatura até expirar o prazo de classificação da informação a que a **CONTRATADA** teve acesso em razão do contrato ao qual se vincula o presente instrumento.

A vigência deste Termo independe do prazo de vigência do contrato assinado.

Cláusula Sétima – DAS PENALIDADES

A quebra do sigilo e/ou da confidencialidade das INFORMAÇÕES, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do contrato ao qual se vincula o presente instrumento. Neste caso, A **CONTRATADA**, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pelo Contratante, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis.

Cláusula Oitava – DISPOSIÇÕES GERAIS

Este TERMO de Confidencialidade é parte integrante e inseparável do CONTRATO nº 095/2025.

Parágrafo Primeiro – Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa-fé, da equidade, da razoabilidade, da economicidade e da moralidade.

Parágrafo Segundo – O disposto no presente TERMO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tal como aqui definidas.

Parágrafo Terceiro - Havendo necessidade legal devido a Programas de Governo, A **CONTRATADA** assume o compromisso de assinar Termo de Sigilo (ou equivalente) adicional relacionado ao Programa, prevalecendo as cláusulas mais restritivas em benefício do **CONTRATANTE**.

Parágrafo Quarto – Ao assinar o presente instrumento, A **CONTRATADA** manifesta sua concordância no sentido de que:

I. O **CONTRATANTE** terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da Contratada;
II. A **CONTRATADA** deverá disponibilizar, sempre que solicitadas formalmente pelo Contratante, todas as informações requeri das pertinentes ao contrato ao qual se vincula o presente termo;

III. A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo;

IV. Todas as condições, TERMOS e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes;

V. O presente TERMO somente poderá ser alterado mediante TERMO aditivo firmado pelas partes;

VI. Alterações do número, natureza e quantidade das informações disponibilizadas para a
CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

VII. O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações disponibilizadas para a **CONTRATADA**, serão incorporados a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas;

VIII. Este TERMO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar INFORMAÇÕES para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

Cláusula Nona – DO FORO

Fica eleito o foro da comarca de Salvador, onde está localizada a sede do **CONTRATANTE**, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO é assinado pelas partes para que produza seus regulares efeitos.

_____, _____ de _____ de 20____

De acordo.

CONTRATANTE

MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA
André Luis Sant´Ana Ribeiro
Superintendente de Gestão Administrativa

CONTRATADA

CENTRO DE PESQUISAS EM INFORMÁTICA LTDA
João Gualberto Rizzo Araújo
sócio – diretor

Documento assinado eletronicamente por **João Gualberto Rizzo Araujo** - Usuário Externo, em 23/07/2025, às 15:44, conforme Ato Normativo n° 047, de 15 de Dezembro de 2020 - Ministério Público do Estado da Bahia.

Documento assinado eletronicamente por **André Luis Sant Ana Ribeiro** - Superintendente, em 24/07/2025, às 10:56, conforme Ato Normativo n° 047, de 15 de Dezembro de 2020 - Ministério Público do Estado da Bahia.

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 **1618719** e o código CRC **D2C9C5FA**.

MINISTÉRIO PÚBLICO
DO ESTADO DA BAHIA

CONTRATO

TERMO DE RERRATIFICAÇÃO AO CONTRATO Nº 095/2054-SGA QUE ENTRE SI CELEBRAM O MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA E QOS TECNOLOGIA E SERVIÇOS LTDA.

Pelo presente instrumento, o **MINISTÉRIO PÚBLICO DO ESTADO DA BAHI**A, pessoa jurídica de direito público, inscrito no CNPJ sob o número 04.142.491/0001-66, com sede situada à 5ª Avenida, nº 750, Centro Administrativo da Bahia – CAB, neste ato representado, mediante Ato de Delegação nº 70/2014, pelo Superintendente de Gestão Administrativa, **Centro de Pesquisas em Informática Ltda**, CNPJ no 40.584.096/0002-88, estabelecida à Av. Santos Dumont, 6216, S331 Quadra única, Loteamento Jardim Santo Antônio, Pitangueiras, Lauro de Freitas/BA, CEP 42.701-260, representada por seu sócio - diretor Sr. **João Gualberto Rizzo Araújo,** inscrito no CPF/MF sob o nº 50*******20, doravante denominada **CONTRATADA**, resolvem rerratificar o contrato nº 095/2025-SGA celebrado entre as partes em 24 de julho de 2025, a fim de consignar o que seque:

CLÁUSULA PRIMEIRA – DO OBJETO

1.1 O presente Termo de rerratificação tem por objeto retificar, em **razão de erro material**, as informações relativas à cláusula **décima quarta "DA GARANTIA DA EXECUÇÃO"**, considerando o quanto previsto no **item 4.1.3.1 do Termo de referência do Edital da Licitação nº 90015/2025:**

☒ **SERÁ EXIGIDA GARANTIA CONTRATUAL.**

4.1.3.1.1 A garantia deverá ser prestada no percentual de 5% (padrão) do valor total inicial do contrato, conforme regras estabelecidas no instrumento contratual.

4.1.3.1.2 A garantia deverá ser prestada em até 10 dias corridos, após a assinatura do contrato.

4.1.3.1.3 A garantia na modalidade seguro-garantia deverá ser prestada em até 10 dias corridos, contados da data da homologação da licitação até no máximo à assinatura do contrato (art. 96, §3° da Lei Federal n° 14.133, de 2021).

4.1.3.1.4 No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser ajustada ou renovada, seguindo os mesmos parâmetros utilizados para a contratação.

4.1.3.1.5 Além da garantia de que tratam os arts. 96 e seguintes da Lei nº 14.133/2021, a contratação possui previsão da garantia de que trata o art. 26 do CDC, incluindo manutenção e assistência técnica, conforme condições estabelecidas neste Termo de Referência.

4.1.3.1.6 A garantia de contratação é independente de eventual garantia do serviço prevista especificamente neste Termo de Referência, nos termos do Código de Defesa do Consumidor (CDC).

CLÁUSULA SEGUNDA – DA RATIFICAÇÃO

Ficam ratificadas todas as demais cláusulas e condições do Contrato nº 095/2025-SGA referido, não alteradas pelo presente instrumento.

E por estarem justos e acordados, o presente é assinado para um só efeito de direito.

CENTRO DE PESQUISAS EM INFORMÁTICA LTDA
João Gualberto Rizzo Araújo
sócio- diretor

MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA
André Luis Sant´Ana Ribeiro
Superintendente de Gestão Administrativa

(Assinado e datado eletronicamente/digitalmente)

Documento assinado eletronicamente por **João Gualberto Rizzo Araujo** - Usuário Externo, em 30/07/2025, às 10:23, conforme Ato Normativo n° 047, de 15 de Dezembro de 2020 - Ministério Público do Estado da Bahia.

Documento assinado eletronicamente por **André Luis Sant Ana Ribeiro** - Superintendente, em 30/07/2025, às 10:42, conforme Ato Normativo n° 047, de 15 de Dezembro de 2020 - Ministério Público do Estado da Bahia.