MINISTÉRIO PÚBLICO
DO ESTADO DA BAHIA

CONTRATO

CONTRATO DE PRESTAÇÃO DE SERVIÇOS QUE, ENTRE SI, CELEBRAM O MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA E A EMPRESA HSC DESENVOLVIMENTO E SERVIÇOS EM TECNOLOGIA DA INFORMAÇÃO LTDA, NA FORMA ABAIXO:

CONTRATO Nº 001/2021 – SGA

O **MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA**, pessoa jurídica de direito público, com sede na 5ª Avenida, 750, Centro Administrativo da Bahia, inscrita no CNPJ sob o Nº 04.142.491/0001-66, doravante denominado **CONTRATANTE**, neste ato representado, mediante Ato de Delegação nº 70/2014, pelo seu Superintendente de Gestão Administrativa, **Frederico Welington Silveira Soares**, e a **EMPRESA HSC DESENVOLVIMENTO E SERVIÇOS EM TECNOLOGIA DA INFORMAÇÃO LTDA**, CNPJ nº. 13.103.980/0001-08, doravante denominada **CONTRATADA**, estabelecida à Rua General João Manoel, 50, 5° andar, sala 502, Centro Histórico, Porto Alegre/RS, representada por seu representante legal **Romulo Giordani Boschetti**, CPF/MF nº. [redacted] **CELEBRAM** o presente Contrato, com supedâneo no quanto disposto na Lei Estadual-BA nº 9.433/2005, e, ainda, observado o constante no Edital de Licitação do tipo menor preço, modalidade Pregão Eletrônico nº 048/2020, protocolado sob o nº SEI 19.09.02684.0007250/2020-58, o qual integra este instrumento independentemente de transcrição, mediante as cláusulas e condições seguintes:

CLÁUSULA PRIMEIRA - DO OBJETO

1.1 Constitui objeto do presente contrato a prestação de serviços gateway de e-mail em nuvem com módulo de inspeção de E-mails entre caixas de correio e serviços online de proteção / filtragem de e-mail para 4.000 caixas postais, com o objetivo de proteção anti-spam, anti-malware, anti-phishing, anti-spear phishing (phishing direcionado), tratamento de ameaças avançadas, incluindo sistema de segurança contra ataques dirigidos, com sandbox para verificar arquivos anexos, assim como suporte técnico, implantação e treinamento, conforme detalhamento descrito neste documento de especificações técnicas detalhadas, pelo período de 24 meses.

1.2 Incluem-se no objeto contratado todos os custos com implantação, treinamento, garantia e suporte técnico pelo período de 24 (vinte e quatro meses), bem como a disponibilização das licenças de uso do software para 3.500 caixas postais existentes;

CLÁUSULA SEGUNDA – DA FORMA DE FORNECIMENTO, DA ENTREGA E DO RECEBIMENTO

2.1 O Regime de execução do presente instrumento é de Empreitada por Preço Global;

2.2 A **CONTRATADA** deverá diligenciar a disponibilização (habilitação) da solução no prazo de 05 (cinco) dias contados da data da entrega da Nota de Empenho acompanhada do instrumento contratual;

2.3.1 A comprovação da habilitação se dará mediante comunicação notificação da empresa ao **CONTRATANTE** através do e-mail da Coordenação de Assessoramento em Segurança da Informação - casi@mpba.mp.br, informando da disponibilização do acesso ao serviço contratado.

2.4 Antes do início da execução dos serviços de migração e implantação, deverá a **CONTRATADA**, com apoio da equipe da Diretoria de Tecnologia da Informação (DTI) do **CONTRATANTE**, planejar todas as ações a serem tomadas durante a execução dos serviços inerentes ao objeto contratual, em um prazo de até 10 (dez) dias após a habilitação da solução, conforme descrito no item 2.3.1;

2.5 Todas as tarefas administrativas estão previstas para ocorrerem em horário comercial, de segunda-feira a sexta-feira das 08:00 h às 18:00 h, podendo ocorrer atividades fora do horário comercial mediante autorização do **CONTRATANTE**.

2.6 A **CONTRATADA** fornecerá o treinamento nas tecnologias da solução especificada neste instrumento para até 05 (cinco) técnicos da equipe do **CONTRATANTE**, em formato **HANDS ON**, no prazo de 15 (quinze) dias contados da data da migração e implantação da solução, cujo escopo deverá abordar as funcionalidades de cada tecnologia, atendendo aos seguintes critérios:

2.6.1 O treinamento será realizado de forma remota (EAD), disponibilizado no período acordado entre as partes;

2.6.2 Abrangerá configuração de regras, políticas etc, com carga horária mínima de 16 (dezesseis) horas;

2.6.3 Deverá ser ministrado em dias úteis, em meio período (matutino ou vespertino), conforme definido pelo CONTRATANTE;

2.6.4 O conteúdo programático do curso deverá ser previamente aprovado pelo CONTRATANTE;

2.6.4.1 Eventuais alterações no conteúdo a ser ministrado deverão ser aprovadas previamente pelo CONTRATANTE, respeitando-se, minimamente, a abrangência de todas as funcionalidades nativas da solução assim como as customizáveis a serem implantadas.

2.6.5 O treinamento será ministrado por profissional certificado pelo fabricante da solução, devendo ser o mesmo disponibilizado diretamente pelo fabricante ou compor o quadro de funcionários da CONTRATADA, a critério desta;

2.7 O prazo total para entrega, implantação, treinamento e plena operacionalização da solução é de 30 (trinta) dias, contados da data da entrega do empenho, nos termos do item 2.3 deste instrumento;

2.8 **CONTRATANTE** rejeitará, no todo ou em parte, o objeto contratual em desacordo com as condições pactuadas, podendo, entretanto, se lhe convier, decidir pelo recebimento, neste caso com as deduções cabíveis;

2.9 O recebimento provisório do objeto contratual se dará no prazo de 05 dias contados da data da habilitação da solução, observadas as disposições constantes dos **itens 2.3 e 2.3.1**;

2.10 O recebimento definitivo do objeto deste contrato só será concretizado depois de adotados, pelo **CONTRATANTE**, todos os procedimentos administrativos cabíveis, observados os termos do art. 161 da Lei Estadual nº 9.433/2005.

2.10.1 O recebimento definitivo far-se-á mediante termo circunstanciado, no prazo de até 30 (trinta) dias, e ficará sob a responsabilidade do fiscal do contrato em conjunto com Comissão de Recebimento do CONTRATANTE designada pela Portaria nº 284/2019-SGA, ou por instrumento que eventualmente a substitua, na hipótese de o valor contratual exceder o limite legal previsto para a realização de licitações na modalidade convite;

2.11 O aceite ou aprovação do objeto pelo CONTRATANTE não exclui a responsabilidade civil e/ou administrativa da CONTRATADA por vícios, defeitos ou disparidades com as especificações estabelecidas neste Contrato e no processo de Licitação que o originou, verificadas posteriormente, garantindo-se ao CONTRATANTE, inclusive, as faculdades previstas na Lei Federal n.º 8.078/90 – Código de Defesa do Consumidor.

CLÁUSULA TERCEIRA - DA DOTAÇÃO ORÇAMENTÁRIA

As despesas para o pagamento deste contrato correrão por conta dos recursos da Dotação Orçamentária a seguir especificada:

Cód. Unidade Orçamentária/Gestora	Destinação de Recursos (Fonte)	Ação (P/A/OE)	Região	Natureza da Despesa
40.601.0003	100	2002	9900	33.90.40

CLÁUSULA QUARTA - DO PREÇO

4.1 Dá-se ao presente contrato o valor total de R$ 469.000,00 (quatrocentos e sessenta e nove mil reais).

4.2 Nos preços computados neste Contrato estão inclusos todos e quaisquer custos necessários ao fiel cumprimento deste instrumento, inclusive todos aqueles relativos a remunerações, encargos sociais, previdenciários e trabalhistas de todo o pessoal disponibilizado pela **CONTRATADA** para a execução do objeto contratado, implantação, ativação, instalação, configuração, customização, transportes de qualquer natureza, deslocamentos, viagens, embalagem, ferramentas, materiais e insumos empregados, depreciação, aluguéis, administração, tributos e emolumentos.

CLÁUSULA QUINTA – DOS ACRÉSCIMOS E SUPRESSÕES

5.1 A **CONTRATADA** se obriga a aceitar, quando solicitado e devidamente motivado pela Administração, nas mesmas condições estabelecidas neste instrumento, os acréscimos ou supressões de até 25% (vinte e cinco por cento) do valor inicial atualizado do contrato, na forma do § 1º do art. 143 da Lei Estadual-BA nº 9.433/2005;

5.2 As supressões poderão ser superiores a 25% (vinte e cinco por cento), desde que haja resultado de acordo entre os contratantes.

CLÁUSULA SEXTA - DAS CONDIÇÕES DE PAGAMENTO E DA RETENÇÃO DE TRIBUTOS

6.1 O faturamento referente ao objeto deste contrato será efetuado em parcela única, após o recebimento definitivo do objeto, e o pagamento será processado mediante apresentação, pela **CONTRATADA**, da Nota Fiscal, devidamente acompanhada do **ACEITE** pelo **CONTRATANTE** e das certidões cabíveis, e se concluirá no prazo de 08 (oito) dias úteis a contar da data de apresentação da documentação, desde que não haja pendência a ser regularizada;

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

6.2 As notas fiscais far-se-ão acompanhar da documentação probatória relativa ao recolhimento dos tributos que tenham como fato gerador o objeto consignado na **CLÁUSULA PRIMEIRA**;

6.3 O **CONTRATANTE** realizará a retenção de impostos ou outras obrigações de natureza tributária, nas hipóteses em que figurar como substituto tributário;

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

6.5 A atualização monetária dos pagamentos devidos pelo **CONTRATANT**E, em caso de mora, será calculada considerando a data do vencimento da obrigação e do seu efetivo pagamento, de acordo com a variação do INPC do IBGE pro rata tempore, observado, sempre, o disposto no item **6.1.1**.

CLÁUSULA SÉTIMA – DA MANUTENÇÃO DAS CONDIÇÕES DA PROPOSTA, DO REAJUSTAMENTO E DA REVISÃO DE PREÇOS

7.1 Considerando-se as especificidades da presente contratação, de modo que o valor pago pelo contratante contempla o valor global para o prazo de 24 meses, a concessão de reajustamento deverá observar o seguinte:

7.1.1 O valor contratado é irreajustável durante a vigência inicial do contrato;

7.1.2 Apenas será cabível na hipótese de prorrogação do prazo de vigência do contrato, nos termos dispostos na cláusula oitava, mediante requerimento da **CONTRATADA**;

7.1.3 Será calculado com base na aplicação do INPC/IBGE acumulado no período compreendido entre a data da apresentação da proposta, qual seja, 07/12/2020 e a data do 2º aniversário da mesma, observadas as disposições legais;

7.1.4 A variação do valor contratual para fazer face ao reajuste de preços não caracteriza alteração do mesmo, podendo ser registrada por simples apostila, dispensando a celebração de aditamento;

7.1.5 Quando, antes da data do reajustamento, tiver ocorrido revisão do contrato para manutenção do seu equilíbrio econômico financeiro, exceto nas hipóteses de força maior, caso fortuito, agravação imprevista, fato da administração ou fato do príncipe, será a revisão considerada à ocasião do reajuste, para evitar acumulação injustificada.

7.2 A revisão de preços nos termos do inc. XXVI do art. 8º da Lei Estadual nº. 9.433/2005, por interesse da **CONTRATADA**, dependerá de requerimento formal, instruído com a documentação que comprove o desequilíbrio econômico-financeiro do Contrato. Deverá ser instaurada pelo **CONTRATANTE**, entretanto, quando este pretender recompor o preço que se tornou excessivo;

7.2.1 A revisão de preços, se ocorrer, deverá ser formalizada através de celebração de Aditivo Contratual.

CLÁUSULA OITAVA - DA VIGÊNCIA

8.1 O presente contrato vigerá por 25 (vinte e cinco) meses, a contar da data da sua publicação no Diário da Justiça Eletrônico, admitindo-se a sua prorrogação, por até 48 (quarenta e oito) meses, nos termos do artigo 140, III, da Lei Estadual/BA nº 9.433/2005, e desde que formalizada mediante termo aditivo.

8.2 Caso o prazo de validade do licenciamento objeto deste contrato ultrapasse a vigência do ajuste, as obrigações contratualmente estabelecidas permanecem válidas e eficazes, inclusive no que toca às prerrogativas administrativas ora estabelecidas em favor do **CONTRATANTE**, ainda que encerrado o lapso temporal de vigência do instrumento contratual.

CLÁUSULA NONA – DA GARANTIA, SUPORTE TÉCNICO E NÍVEIS DE SERVIÇO (SLA)

9.0 A **CONTRATADA** fornecerá os objetos deste contrato com garantia mínima de 24 (vinte e quatro) meses, contados a partir do recebimento do objeto, conforme **CLÁUSULA SEGUNDA** deste instrumento, conforme condições a seguir especificadas:

9.1 O período da subscrição de uso da solução de Antispam em nuvem será de 24 (vinte e quatro) meses, com suporte técnico presencial de 8 (oito) horas por dia, 5 (cinco) dias por semana, na cidade de Salvador (BA);

9.1.1 Durante o período da subscrição o fabricante deverá garantir o funcionamento da solução, com suporte técnico prestado em caso de falha;

9.1.2 Deverá garantir durante o período de subscrição atualização de versões, releases, componentes (bibliotecas, filtros etc.) e demais itens que se façam necessários ao pleno funcionamento da solução.

9.2 A **CONTRATADA** deverá possuir equipe de técnicos certificados pelo fabricante do software fornecido, e preparada para dar todo o suporte técnico e ajuda necessária para maximizar os benefícios oferecidos pelo software, aumentando a sua performance;

9.2.1Todo suporte deve ser prestado por técnicos certificados pelo fabricante.

9.3 A **CONTRATADA** deverá prestar suporte a todos os componentes de software fornecidos que forem necessários para a implementação e utilização da solução, sem ônus para o **CONTRATANTE** durante 24 (vinte e quatro) meses.

9.4 A **CONTRATADA** deverá realizar uma análise da situação atual e elaborar, em conjunto com a equipe interna do **CONTRATANTE**, um plano de otimização de recursos, rotinas, procedimentos e processos para o novo ambiente de segurança. Essa documentação deverá ser entregue, pela **CONTRATADA**, em formato digital.

9.5 A **CONTRATADA** deverá preparar o ambiente de modo a operar conforme o estabelecido no plano de otimização de recursos, rotinas, procedimentos e processos.

9.6 A **CONTRATADA** deverá preservar todo ambiente computacional existente, de forma a manter a integridade dos dados, aplicativos e sistemas operacionais em funcionamento.

9.7 A instalação e configuração da solução deverá ser realizada de acordo com o horário de funcionamento do **MPBA**, de segunda à sexta-feira, das 8:00 às 18:00h, em horário e dia a serem combinados entre a **MPBA** e a **CONTRATADA**;

9.8 A instalação e configuração dos softwares adquiridos deverão ser executadas em 100% do Parque **CONTRATANTE**, localizado em Salvador (BA);

9.9 A **CONTRATADA** deverá realizar, durante o período de vigência do contrato, no mínimo, e mediante solicitação do **CONTRATANTE**, duas avaliações do ambiente do Ministério Público do Estado da Bahia, mediante verificação de instalações e configurações de toda a solução, adequando-as às melhores práticas. Esta atividade deverá gerar relatório a ser entregue ao **CONTRATANTE** para análise de melhorias pela equipe da Diretoria de Tecnologia da Informação do **CONTRATANTE**.

9.2 O serviço de Assistência Técnica será prestado a fim de atender às necessidades do **CONTRATANTE** para suporte técnico do software de Visibilidade, Conformidade, Controle de Acesso e Segurança, com o objetivo de controlar o acesso de dispositivos à rede corporativa e aumentar o nível de conformidade com a política de segurança;

9.2.1 A **CONTRATADA** deverá possuir Central de Atendimento (contato telefônico, sitio na Internet e e-mail) para consultas, aberturas de chamados técnicos e envio de arquivos para análise, durante 08 (oito) horas por dia, 5 (cinco) dias por semana.

9.2.2 A **CONTRATADA** deverá prestar serviços de suporte técnico 08 (oito) horas por dia, 5 (cinco) dias por semana, na cidade de Salvador (BA), sem ônus para o **CONTRATANTE**;

9.2.3 A abertura de chamados para a Assistência Técnica deve ser realizada mediante os seguintes canais: telefone, e-mail e web site, os quais deverão estar disponíveis no regime 8 x 5 (oito horas e cinco dias por semana) e deverão ser informados ao **CONTRATANTE**;

9.2.4 Eventuais atrasos que comprometam o prazo de resolução dos problemas deverão ser renegociados com o **CONTRATANTE**. Caso o **CONTRATANTE** entenda que os motivos expostos não justificam os atrasos, a CONTRATADA estará sujeita às sanções legais previstas;

9.2.5 Sempre que for solicitado, a **CONTRATADA** deve fornecer uma relação dos chamados técnicos gerados pela **CONTRATANTE**, os quais constarão, pelo menos: status do chamado, descrição do problema, datas e prazos de atendimento, descrição da solução e responsável técnico;

9.2.6 Após o início do atendimento técnico, a **CONTRATADA** somente dará por encerrado o chamado mediante a inspeção dos serviços e o respectivo aceite da **CONTRATANTE**;

9.2.7 Em todas as atividades de assistência técnica ou suporte, os técnicos da deverão empregar a Língua Portuguesa, exceto no uso de termos técnicos e na utilização de textos técnicos, que poderão estar redigidos em Língua Inglesa.

9.2.8 Caberá ao **CONTRATANTE** requisitar o suporte técnico, ficando a **CONTRATADA** obrigada a realizá-lo, de acordo com o nível de severidade e nos prazos máximos estabelecidos neste instrumento;

9.2.9 Todos os chamados, inclusive os que podem resultar em manutenção de natureza corretiva, bem como o fluxo de resolução de problemas, deverão ser documentados. Esta documentação, bem como outras geradas em processos de atendimento, auditorias, manutenção ou configurações, deverá ser entregue à **CONTRATANTE** através de relatórios (impressos ou em mídia digital) mediante solicitação;

9.2.10 A **CONTRATADA** deverá fazer análises dos chamados e enviar recomendações de possíveis treinamentos necessários ao desenvolvimento da equipe da **CONTRATANTE**;

9.2.11 A **CONTRATADA** deverá apresentar relatório contendo as ações adotadas para a solução do problema;

9.2.12 O marco inicial para contagem do prazo de início de atendimento é a abertura do chamado registrada através dos meios exigidos neste instrumento;

9.3 Para efeito dos atendimentos técnicos, a **CONTRATADA** deverá observar os seguintes níveis de serviços:

9.3.1 Disponibilização de Plantão Telefônico por número 0800 como serviço de uso ilimitado, no período de 8 (oito) horas por dia, 5 (cinco) dias por semana;

9.3.2 Atendimento No Local (Onsite) – 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 da **CONTRATANTE**.

9.3.3 A solução de problemas deverá atender no mínimo os níveis de serviço abaixo:

Disponibilidade do serviço	99,99% de uptime
Proteção contra Vírus	Nenhum E-mail com vírus
Efetividade no bloqueio de SPAM	99% ou maior
Ocorrência de Falsos-positivos	Não mais que 0,0003%
Latência máxima na entrega de mensagens	Não mais que um minuto
Efetividade do Suporte	Tempo de atendimento baseado na criticidade do chamado.

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

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**	**Níveis de Severidade**		
		1	**2**	**3**
Onsite	Início atendimento	1 hora	2 horas	24 horas
	Término atendimento	2 horas	4 horas	72 horas
Telefone, e-mail e web	Início atendimento	---	---	24 horas
	Término atendimento	---	---	72 horas

9.3.4.1 Para o Nível 1, caso o atendimento não seja finalizado até as 20h00min, o técnico não poderá interrompê-lo, devendo continuar até sua finalização, ou a interrupção do mesmo pela Coordenação de Tecnologia e Gestão da Informação. Todo o chamado somente será caracterizado como "encerrado" mediante concordância da Coordenação de Tecnologia e Gestão da Informação.

9.3.4.2 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**.

9.3.4.3 A **CONTRATADA** deverá disponibilizar ao **CONTRATANTE** um serviço preventivo de verificação e atualização de versões ou correções (patches) que se fizerem necessários, específicos para a solução ofertada, sem ônus para o **CONTRATANTE**.

9.3.4.4 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, sem ônus para o **CONTRATANTE**.

9.4 A **CONTRATADA** deverá disponibilizar ao **CONTRATANTE** serviço de atendimento de um Gestor do contrato de Suporte, responsável este que será o ponto focal de todas as necessidades de suporte do **CONTRATANTE** para casos de escalações ou problemas de atendimento do Suporte Técnico. Caso a **CONTRATADA** tenha seus laboratórios em outros países que não seja o território nacional, o Gestor deverá ter fluência na língua para facilitar a comunicação entre as partes.

9.5 O **CONTRATANTE** permitirá o acesso dos técnicos credenciados pela **CONTRATADA** às instalações onde se encontrarem os equipamentos para a prestação dos serviços de manutenção. Entretanto, tais técnicos ficarão sujeitos às normas internas de segurança do **CONTRATANTE**, notadamente àquelas atinentes à identificação, trânsito e permanência nas dependências.

9.6 A permanência de técnico em atendimento além do tempo previsto para resolução do problema, ainda quando autorizado pelo **CONTRATANTE**, não deverá representar qualquer ônus adicional ao mesmo;

9.7 A **CONTRATADA** deverá ainda realizar os seguintes suportes proativos:

9.7.1 Duas avaliações on-site por ano do ambiente do **CONTRATANTE**, mediante verificação de instalações e configurações de toda a solução, adequando-as às melhores práticas de segurança, essa atividade deve gerar relatório para posterior melhoria pela equipe do **CONTRATANTE**.

9.7.2 Uma avaliação on-site por ano do ambiente do **CONTRATANT**E, mediante verificação de instalações e configurações de toda a solução de gerência centralizada, adequando-as às melhores práticas de segurança, essa atividade deve gerar relatório para posterior melhoria pela equipe do **CONTRATANTE**.

9.7.3 Quatro visitas técnicas on-site durante o ano de profissionais certificados pelo fabricante para apoiar nas implementações e nos controles gerados pelas ações proativas.

9.8 Eventuais despesas com deslocamento de técnicos aos locais de execução dos serviços, bem como todas as despesas de transporte, diárias, tributos, seguros ou qualquer despesa envolvida na execução contratual são de responsabilidade exclusiva da **CONTRATADA**.

CLÁUSULA DÉCIMA – DAS OBRIGAÇÕES DA CONTRATADA

10 Além das determinações contidas no instrumento convocatório e no presente contrato, bem como daquelas decorrentes de lei, a **CONTRATADA**, obriga-se a:

10.1 Fornecer e implantar a solução contratada de acordo com as especificações técnicas constantes no instrumento convocatório e no presente contrato, no local determinado, nos dias e nos turnos e horários de expediente do **CONTRATANTE**, respeitando todos os prazos estipulados, não podendo eximir-se da obrigação, ainda que parcialmente, sob a alegação de falhas, defeitos ou falta de materiais, pessoal e/ou peças;

10.2 Dimensionar adequadamente o quantitativo de recursos necessários para a perfeita execução dos serviços;

10.3 Transferir conhecimento à equipe de TI do **CONTRATANTE**, para que esta possa compreender as particularidades técnicas dos itens fornecidos e prestar assessoramento aos usuários finais;

10.4 Prover capacidade operacional suficiente para plena prestação dos serviços objeto deste instrumento;

10.5 Acompanhar e informar sobre as atualizações tecnológicas necessárias nos produtos e/ou serviços adquiridos, realizando as ações necessárias para a implantação dessas atualizações em comum acordo com o **CONTRATANTE**, até o final do contrato, sem ônus para o **CONTRATANTE**;

10.4 Instalar e configurar todos os softwares que se fizerem necessários para a execução contratual;

10.4.1 Qualquer instalação de software em ambiente do **CONTRATANTE** será precedida de justificativa, e somente será autorizado se for compatível com as exigências do **CONTRATANTE** e de seu provedor. Necessidades outras, além das descritas, serão arcadas pela própria **CONTRATADA**, as quais não serão passíveis de cobranças adicionais.

10.6 Entregar ao **CONTRTANTE** toda e qualquer documentação gerada em função da prestação de serviços decorrente desta contratação;

10.7 Prestar as informações e os esclarecimentos que venham a ser solicitados pelos técnicos do **CONTRATANTE**;

10.8 Reportar formal e imediatamente ao **CONTRATANTE** quaisquer problemas, anormalidades, erros e irregularidades que possam comprometer a execução dos serviços;

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

10.10 Respeitar e fazer com que seus empregados respeitem as normas gerais de segurança do trabalho, identificação, disciplina e outros regulamentos instituídos pelo **CONTRATANTE**, bem como atentar para as regras de cortesia no local onde serão entregues e implantados os bens objeto deste Contrato;

10.11 Promover o imediato afastamento, da execução do objeto contratual, de empregados e/ou prepostos cuja permanência se demonstre em desacordo com este instrumento, ou, ainda, com a moralidade e a ética, correndo, por exclusiva conta da **CONTRATADA**, quaisquer ônus decorrentes das leis trabalhistas e previdenciárias, bem como qualquer outra que tal fato imponha;

10.12 Responsabilizar-se pelo cumprimento das exigências previstas na legislação profissional específica e pelos encargos fiscais e comerciais resultantes da execução do contrato;

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

10.13 Emitir notas fiscais/faturas de acordo com a legislação, contendo descrição dos bens e serviços (quando couber), indicação de quantidades, preços unitários e valor total;

10.14 Arcar, quando da execução do objeto contratual, com todo e qualquer dano ou prejuízo, independentemente da natureza, causado ao **CONTRATANTE** e/ou a terceiros, ainda que por sua culpa, em consequência de erros, imperícia própria ou de auxiliares que estejam sob sua responsabilidade, bem como ressarcir ao **CONTRATANTE** todos os custos decorrentes de paralisação ou interrupção da execução do objeto contratado, exceto quando isto ocorrer por sua solicitação, ou ainda por caso fortuito ou força maior, desde que tais circunstâncias sejam formalmente comunicadas ao **CONTRATANTE** no prazo de até 48 (quarenta e oito) horas após a sua ocorrência;

10.15 Providenciar e manter atualizadas todas as licenças e alvarás junto às repartições competentes que, porventura, sejam necessários à execução do contrato;

10.16 Não introduzir, seja a que título for, nenhuma modificação na especificação do objeto contratado, sem o consentimento prévio, e por escrito, do **CONTRATANTE**;

10.17 Atender com presteza às reclamações sobre a qualidade dos bens e serviços e/ou inexecução do contrato, providenciando sua imediata reparação, substituição e/ou realização, sem ônus para o **CONTRATANTE**;

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

10.18.1 A **CONTRATADA** se obriga a permitir que a auditoria interna do **CONTRATANTE** e/ou auditoria externa por ela indicada tenham acesso a todos os documentos que digam respeito à execução contratual;

10.19 Garantir que todos os seus sócios, gestores, administradores e/ou funcionários mantenham sigilo absoluto sobre quaisquer informações, dados, documentos e assuntos que tomarem conhecimento em razão da execução do objeto contratual, sob pena de responsabilização civil, administrativa e/ou penal, nos termos da legislação vigente,

10.19.1 Deverá a **CONTRATADA**, como condição para assinatura deste instrumento, firmar o **TERMO DE COMPROMISSO**, **SIGILO E CONFIDENCIALIDADE** constante no **APENSO II** deste contrato.

CLÁUSULA DÉCIMA PRIMEIRA - DAS OBRIGAÇÕES DO CONTRATANTE

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

11.1 Fornecer, no prazo de 10 (dez) dias a contar da data da assinatura do contrato, as informações necessárias para que a **CONTRATADA** possa executar plenamente o objeto contratado;

11.2 Realizar os pagamentos devidos pela execução do contrato, nos termos e condições previstos nas **CLÁUSULAS QUARTA E SEXTA**;

11.3 Proporcionar todas as condições necessárias para que a **CONTRATADA** possa cumprir as obrigações assumidas no contrato.

11.4 A fornecer acesso aos ambientes para implantação das soluções;

11.5 Disponibilizar todas as informações necessárias para o desenvolvimento dos trabalhos;

11.6 Acompanhar e fiscalizar o fiel cumprimento dos prazos e das condições de realização do presente contrato, notificando a **CONTRATADA**, por escrito, sobre imperfeições, falhas ou irregularidades constatadas na execução do objeto, para que sejam adotadas as medidas corretivas necessárias;

11.7 Validar, aprovar e realizar os pagamentos referentes aos serviços prestados, nos termos do contrato firmado entre as partes.

11.8 Fornecer à **CONTRATADA**, mediante solicitação, atestado de capacidade técnica, quando o fornecimento do objeto atender satisfatoriamente os prazos de entrega, qualidade e demais condições previstas neste Contrato.

CLÁUSULA DÉCIMA SEGUNDA - DA FISCALIZAÇÃO DO CONTRATO

12.1 Na forma das disposições estabelecidas na Lei Estadual-BA nº 9.433/2005, o **CONTRATANTE** designará servidor(es), **por meio de Portaria específica para tal fim**, para a fiscalização deste contrato, tendo poderes, entre outros, para notificar a **CONTRATADA** sobre as irregularidades ou falhas que porventura venham a ser encontradas na execução deste instrumento;

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

12.2.1 Acompanhar o cumprimento dos prazos de execução descritos neste instrumento, e anotar, em registro próprio, as ocorrências relativas à execução do contrato, determinando as providências necessárias à correção de falhas, irregularidades e/ou defeitos, podendo ainda suspender-lhes a execução, sem prejuízos das sanções contratuais legais;

12.2.2 Transmitir à **CONTRATADA** instruções, e comunicar alterações de prazos, cronogramas de execução e especificações do projeto, quando for o caso;

12.2.3 Dar imediata ciência a seus superiores dos incidentes e ocorrências da execução que possam acarretar a imposição de sanções ou a rescisão contratual;

12.2.4 Adotar, junto a terceiros, as providências necessárias para a regularidade da execução do contrato;

12.2.5 Promover, com a presença de preposto da **CONTRATADA**, a verificação do fornecimento/serviço já efetuados, emitindo a competente habilitação para o recebimento de pagamentos;

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

12.2.7 Fiscalizar a obrigação da **CONTRATADA** de manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, as condições de habilitação e qualificação exigidas para a contratação, bem como o regular cumprimento das obrigações trabalhistas, previdenciárias, fiscais e comerciais resultantes da execução do contrato;

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

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

12.4 O **CONTRATANTE** poderá recusar, sustar e/ou determinar a substituição de bens ou refazimento de serviços que não estejam sendo ou não tenham sido fornecidos ou executados de acordo com as Normas Técnicas e/ou em conformidade com as condições deste contrato ou do procedimento licitatório que o originou, ou ainda que atentem contra a segurança de terceiros ou de bens;

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

12.4.2 A não aceitação de algum bem ou serviço, no todo ou em parte, não implicará na dilação do prazo de execução, salvo expressa concordância do CONTRATANTE.

12.5 Para fins de fiscalização, o **CONTRATANTE** poderá solicitar à **CONTRATADA**, a qualquer tempo, os documentos relacionados com a execução do presente contrato.

CLÁUSULA DÉCIMA TERCEIRA - DAS PENALIDADES

13.1 A **CONTRATADA** sujeitar-se-á às sanções administrativas previstas na Lei Estadual-BA nº. 9.433/2005, as quais poderão vir a ser aplicadas após o prévio e devido processo administrativo, assegurando-lhe, sempre, o contraditório e a ampla defesa.

13.2 - Em caso de inadimplemento parcial ou total de obrigações pela **CONTRATADA**, e não sendo suas justificativas aceitas pelo **CONTRATANTE**, àquela poderão ser aplicadas, observado o disposto no item anterior, as seguintes penalidades:

13.2.1 Multa;

13.2.2 Suspensão temporária de participação em licitação e impedimento de contratar com a Administração pelo prazo de até 05 (cinco) anos;

13.2.3 Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes desta punição e até que seja promovida sua reabilitação perante a Administração Pública Estadual;

13.2.4 Descredenciamento do sistema de registro cadastral.

13.3 Nas hipóteses de aplicação das sanções previstas nos **itens 13.2.2 a 13.2.4**, estas serão impostas à **CONTRATADA** cumulativamente com multa.

13.4 A inexecução contratual, inclusive por atraso injustificado na execução do contrato, sujeitará o CONTRATADA à multa de mora, que será que será apurada por infração e graduada de acordo com a gravidade da infração, obedecidos os seguintes limites máximos:

13.4.1 - 10% (dez por cento) sobre o valor da nota de empenho ou do Contrato, em caso de descumprimento total da obrigação;

13.4.2 - 0,3% (três décimos por cento) ao dia, até o 30º (trigésimo) dia de atraso, sobre o valor total da parte do fornecimento ou serviço não realizado;

13.4.3 - 0,7% (sete décimos por cento) por cada dia de atraso subseqüente ao 30º (trigésimo), sobre o valor da parte do fornecimento ou serviço não realizado.

13.5. A aplicação de multa à **CONTRATADA** não impede que a Administração rescinda unilateralmente o contrato e aplique as demais sanções previstas na Lei Estadual-BA nº 9.433/2005;

13.6 Quando aplicadas, as multas deverão ser pagas espontaneamente no prazo máximo de 05 (cinco) dias úteis, ou serem deduzidas do pagamento a ser efetuado pelo **CONTRATANTE**, caso este deva ocorrer dentro daquele prazo;

13.6.1 Na hipótese de ausência de adimplemento voluntário e impossibilidade de dedução, as multas poderão ser cobradas judicialmente, a critério do **CONTRATANTE**;

13.7 A aplicação de multas não tem caráter compensatório, e o seu pagamento não eximirá a **CONTRATADA** da responsabilidade por perdas e/ou danos decorrentes das infrações cometidas;

13.8 Os custos correspondentes a danos e/ou prejuízos causados por culpa ou dolo da **CONTRATADA** deverão ser ressarcidos ao **CONTRATANTE** no prazo máximo de 05 (cinco) dias úteis, contados da notificação administrativa, sob pena de, sem prejuízo do ressarcimento, serem considerados como hipótese de inadimplemento contratual, sujeita, portanto, à aplicação das sanções administrativas previstas nesta Cláusula.

CLÁUSULA DÉCIMA QUARTA – DA RESCISÃO

14.1 A inexecução total ou parcial do Contrato ensejará a sua rescisão, com as consequências contratuais previstas no Capítulo IX, Seção VIII - Da Inexecução e da Rescisão dos Contratos, da Lei Estadual-BA nº 9.433/2005;

14.2 O **CONTRATANTE** poderá rescindir unilateral e administrativamente o presente Contrato, nas hipóteses previstas nos incisos I a XVI, XX e XXI do art. 167 da Lei Estadual-BA nº 9.433/2005.

14.3 Havendo rescisão administrativa do presente contrato, baseada em alguma das hipóteses previstas nos incisos II a XII do art. 167 da Lei Estadual-BA nº 9.433/2005, o **CONTRATANTE** poderá adotar, no que couber, as medidas que vão a seguir discriminadas:

14.3.1 Assunção imediata do objeto do Contrato, no estado e local em que se encontrar, por ato próprio do **CONTRATANTE**;

14.3.2 Ocupação e utilização de locais, instalações, equipamentos, materiais e pessoal empregados na execução do Contrato, necessários à sua continuidade, na forma prevista na legislação em vigor;

14.3.3 Cobrança dos valores das multas e das indenizações, para ressarcimento da Administração;

14.3.4 Retenção dos créditos decorrentes do contrato até o limite dos prejuízos causados ao **CONTRATANTE**.

CLÁUSULA DÉCIMA QUINTA - DA AUSÊNCIA DE VÍNCULO EMPREGATÍCIO

15.1 A utilização de mão de obra, pela **CONTRATADA**, para execução do presente contrato não ensejará, em nenhuma hipótese, vínculo empregatício com o **CONTRATANTE**.

15.2 Fica garantido o direito de regresso do **CONTRATANTE**, perante a **CONTRATADA**, para ressarcimento de toda e qualquer despesa trabalhista, previdenciária ou correlata que venha a ser condenado a pagar, na eventual hipótese de vir a ser demandado judicialmente por qualquer empregado ou preposto da **CONTRATADA** relativamente à execução do objeto contratual.

CLÁUSULA DÉCIMA SEXTA – DA PROPRIEDADE INTELECTUAL

16.1 A **CONTRATADA** concorda que os direitos patrimoniais autorais relativos aos resultados produzidos em decorrência da execução do objeto contratual são de propriedade exclusiva do **CONTRATANTE**, devidamente amparada pela Lei nº 9.610/1998, de Diretos Autorais, respeitados os direitos morais do autor.

16.2 Entendem-se por resultados quaisquer estudos, relatórios, especificações, descrições técnicas, protótipos, dados, esquemas, plantas, desenhos, diagramas, páginas na Intranet e Internet e documentação didática em papel ou em mídia eletrônica, e-mails. A **CONTRATADA** fica proibida de veicular e comercializar todos e quaisquer produtos e informações geradas ou conhecidas relativas ao objeto da prestação dos serviços, salvo se houver a prévia autorização por escrito do **CONTRATANTE**.

CLÁUSULA DÉCIMA SÉTIMA - DA VINCULAÇÃO AO INSTRUMENTO CONVOCATÓRIO

Integram o presente contrato, como se nele estivessem transcritas, as cláusulas e condições estabelecidas no edital constante no processo licitatório que o originou, referido no preâmbulo deste instrumento, bem como na proposta da **CONTRATADA** apresentada na referida licitação, naquilo em que não divirja deste instrumento.

CLÁUSULA DÉCIMA OITAVA – DA GARANTIA CONTRATUAL

18.1 A CONTRATADA deverá apresentar ao **CONTRATANTE**, no prazo máximo de 10 (dez) dias contados da assinatura do contrato, garantia de 5% (cinco por cento) do valor do contrato, podendo optar por uma das modalidades previstas no parágrafo 1º do art. 136 da Lei Estadual nº 9.433/2005.

18.1.2 A ausência de apresentação da garantia e respectivo comprovante de quitação (conforme o caso) pela **CONTRATADA**, no prazo estipulado nesta cláusula, se configura como hipótese de pendência impeditiva do pagamento, nos termos da **CLÁUSULA SEXTA** deste instrumento, sem prejuízos das sanções contratuais e legais aplicáveis à matéria, em especial o artigo 167, incisos III e X da Lei Estadual/BA nº 9.433/2005;

18.2 A garantia, em qualquer das modalidades, responderá pelo inadimplemento das obrigações contratuais e pelas multas impostas, independentemente de outras cominações legais;

18.2.1 A **CONTRATADA** fica obrigada a, durante toda a vigência do contrato, reforçar o valor vigente da garantia sempre que esta for utilizada para o adimplemento de obrigações e/ou multas;

18.3 Caso haja a celebração de aditivo/apostilamento contratual que enseje acréscimo ao valor contratado, a **CONTRATADA** fica obrigada a complementar a garantia, em igual proporção, antes da consagração do aditamento/apostila;

18.3.1 Nos termos do art. 20 do Decreto Estadual nº 13.967/2012, na hipótese de a **CONTRATADA** se negar a efetuar o reforço da garantia, dentro de 10 (dez) dias contados da data de sua convocação, será aplicada multa no percentual de 2,5% (dois e meio por cento) incidente sobre o valor global do contrato;

18.4 A garantia, quando prestada nas modalidades seguro-garantia ou fiança bancária, deverá ser emitida por instituição devidamente habilitada/credenciada pelo Banco Central para tal mister, e contemplar todo o período de execução do contrato, desde o início de sua vigência até o exaurimento completo do período de 24 (vinte e quatro) meses de licenciamento/atualização contratado;

18.4.1 A garantia prestada em quaisquer das modalidades descritas neste item somente será aceita se contemplar todos os eventos indicados no item 18.6;

18.5 A garantia, quando prestada na modalidade caução, somente será restituída à **CONTRATADA**, no montante a que esta fizer jus, após a finalização total da execução do contrato, observadas as regras impeditivas de pagamento constantes na **CLÁUSULA OITAVA**;

18.5.1 A garantia, quando prestada em dinheiro, será atualizada monetariamente na oportunidade de sua devolução pelo **CONTRATANTE**, segundo critérios da instituição bancária onde se procedeu ao depósito;

18.6 A garantia, qualquer que seja a modalidade escolhida, assegurará o pagamento de:

18.6.1 Prejuízos advindos do não cumprimento do objeto do contrato;

18.6.2 Prejuízos diretos causados ao **CONTRATANTE** decorrentes de culpa ou dolo durante a execução do contrato;

18.6.3 Multas moratórias e punitivas aplicadas pelo **CONTRATANTE** à **CONTRATADA**;

18.6.4 Obrigações trabalhistas e previdenciárias de qualquer natureza, não adimplidas pela **CONTRATADA**, quando couber;

CLÁUSULA DÉCIMA NONA – DA PUBLICIDADE

O **CONTRATANTE** será responsável pela publicação do resumo deste instrumento no Diário da Justiça Eletrônico (DJ-e), do Poder Judiciário do Estado da Bahia, no prazo de 10 (dez) dias corridos, contados a partir da sua assinatura.

CLÁUSULA VIGÉSIMA - 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 PRIMEIRA - DAS DISPOSIÇÕES GERAIS

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

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

21.3 Aplicar-se-á a Lei Estadual nº 9.433/2005 para dirimir toda e qualquer questão legal relativa à execução deste contrato, em especial os casos omissos.

21.4 Fica assegurado ao **CONTRATANTE** o direito de alterar unilateralmente o contrato, mediante justificação expressa, nas hipóteses previstas no inciso I do art. 143 da Lei Estadual nº 9.433/2005, 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**.

21.5 Não caracterizam novação eventuais variações do valor contratual resultantes de reajustamento e/ou 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.

21.6 Inexistindo disposição específica, as obrigações contratuais devem ser praticadas no prazo de 05 (cinco) dias.

E, por assim estarem justos e contratados, firmam o presente Contrato em 02 (duas) vias de igual teor e forma, para que produza seus efeitos legais, após a publicação na Imprensa Oficial.

Salvador, _____ de _____ de 2021.

Ministério Público do Estado da Bahia **Frederico Welington Silveira Soares** Superintendente de Gestão Administrativa	**Empresa Hsc Desenvolvimento e Serviços em Tecnologia da Informação Ltda** **Romulo Giordani Boschetti** Representante legal

APENSO I

Especificação Técnica para Solução de Segurança de e-mail

1. Especificações Técnicas

1.1. Características da Nuvem:

1.1.1. A solução tem que ter garantia de 99,99% de *uptime*;

1.1.2. Por ser de arquitetura em Nuvem, a implantação da solução tem que ser simples, necessitando apenas do apontamento do MS (DNS) para a solução a ser contratada.

1.2. Plataforma de Proteção Avançada em Cloud para E-mails.

1.2.1. A solução deverá ser capaz de permitir a Filtragem baseada em reputação IP para no mínimo: Remetentes permitidos com base no endereço IP, Remetentes bloqueados com base no endereço IP e Bloqueio de e-mails baseados em países e regiões;

1.2.2. A solução deverá permitir a criação de regras/políticas para entrada e saída de e-mails. Permitindo:

1.2.3. Ter a capacidade de processar o tráfego de entrada e de saída de mensagens, com base no IP e domínio de origem da mensagem, permitindo criar filtros e ações diferenciadas para cada sentido;

1.2.4. A criação de regras por:

a. Grupos de usuários;

b. Domínios;

c. Domínios e sufixos (*.ru, *.sk);

d. Range de IP;

e. IP/Rede;

f. Remetentes específicos;

g. Destinatários específicos;

h. Grupos de LDAP.

1.2.5. Tratar e analisar mensagens originadas e recebidas possibilitando a aplicação de regras e políticas customizáveis, além de diferenciadas por sentido de tráfego;

1.2.6. Possibilidade de permitir relay autenticado para clientes externos da corporação;

1.2.7. Deve possuir ferramenta de auditoria de e-mail, com facilidade de pesquisa por origem, destino, assunto e conteúdo da mensagem permitindo a concatenação dos filtros através dos operadores lógicos “e”;

1.2.8. Qualquer aplicação de regras/políticas, inclusive alterações nas já criadas, tem que estar em funcionamento pleno em até 5 (cinco) minutos após sua criação/alteração/deleção.

1.2.9. A solução deverá ser capaz de permitir a filtragem de remetente e destinatários para no mínimo:

1.2.9.1.Remetentes aprovados por endereço de e-mail ou domínio;

1.2.9.2. Remetentes bloqueados por endereço de e-mail ou domínio;

1.2.9.3. Validar destinatário de entrada de e-mail;

1.2.10. A solução deverá ser capaz de detectar spam baseado em assinatura e padrões;

1.2.11. A solução deverá possuir Proteção anti-phishing;

1.2.12. A solução deverá possuir Proteção anti-spear-phishing;

1.2.13. A solução deverá possuir Machine Learning;

1.2.14. A solução deverá possuir Proteção anti- ransomware;

1.2.15. A solução deverá possuir análise de Url’s no corpo do e-mail;

1.2.16. A solução deverá possuir DKIM, DMARC e SPF;

1.2.17. A solução deverá possuir o recurso de analisar a URL antes do clique do usuário;

1.2.18. A solução deverá possuir Proteção contra Comprometimento de E-mail;

1.2.19. A solução deverá possuir Proteção contra-ataques de Engenharia Social, e-mail marketing, e-mail adulto ou qualquer outra forma de ameaça virtual, analisando as mensagens, no mínimo, por meio dos seguintes métodos:

1.2.19.1.Proteção dinâmica por reputação;

1.2.19.2. Assinaturas de spam;

1.2.19.3. Filtros de Vírus:

a. A verificação de vírus, além da técnica tradicional (por assinatura), também deve ser feito através de Big Data do fabricante, bem como utilização de método Fuzzy Hash ou similar para detecção de similaridades e detecção de possível variante de malware;

1.2.19.4. Filtros de anexos;

1.2.19.5. Filtros de phishing;

1.2.19.6. Análise heurística;

1.2.19.7. Análise do cabeçalho, corpo e anexo das mensagens;

1.2.19.8. E-mail bounce;

1.2.19.9. Dicionários pré-definidos e customizados com palavras e expressões regulares;

a. Já deve vir com dicionários pré-estabelecidos, para posterior utilização, tais como:

I. Número de cartão de crédito;

II. CNPJ;

III. CPF e outros;

1.2.20. A solução deverá ser capaz utilizar no mínimo os seguintes bancos de dados de reputação: Known Spam Source (RBL), Dynamically Assigned IP (DUL) e Emerging Threat List (ETL);

1.2.21. A solução deverá possuir um dashboard com informações de Ransomware, Análise em Sandbox, Comprometimento de E-mail, Machine Learning, Spam, Volume de E-mails e Quarentena;

1.2.22. O dashboard deverá permitir a exportação para formatos JPEG, PNG, PDF e CSV;

1.2.23. A solução deverá possuir o Serviço de Banner ou Co-branding (customização do portal com a logo do cliente);

1.2.24. A solução deverá possuir integração com o Active Directory;

1.2.25. A solução deverá permitir o gerenciamento de múltiplos domínios, com aplicação de regras de forma independente para cada um dos domínios;

1.2.26. A solução deverá permitir a integração com Microsoft Office 365, e Servidor de e-mail definido pelo cliente;

1.2.27. A solução deve registrar em log todos os eventos de criação, alterações ou remoção de regras, informando, no mínimo: data e hora do evento, usuário que realizou e quais dados foram alterados;

1.2.28. Deverá possuir um serviço de continuidade de e-mail para que caso o serviço de e-mail do cliente fique fora do ar ou em manutenção a plataforma armazene os e-mails durante 10 dias;

1.2.29. O serviço de continuidade de e-mail deverá fornecer uma caixa de correio para que os usuários possam baixar os e-mails;

1.2.30. A solução AntiSpam deve possuir controle de caixas postais e fluxo de análise de mensagens de no mínimo 500 mensagens por minuto;

1.2.31. Deve ser uma solução MTA (Mail Transfer Agent) completa com suporte ao protocolo SMTP, que controla o envio e o recebimento de todas as mensagens da empresa, com registro de logs das atividades do MTA;

1.2.32. Licenciada para 4000 (quatro mil) caixas postais;

1.2.33. Licença de uso da solução deve possuir 24 meses de subscrição, permitindo atualização, suporte do fabricante compreendendo os seguintes módulos:

1.2.33.1. Atualização das assinaturas de segurança disponibilizadas automaticamente como por exemplo: assinaturas de vírus, malwares e outras ameaças, serviços de reputação de websites, IPs e assinaturas de Websites e aplicativos web;

1.2.33.2. Direito de uso da versão mais atual da solução em cloud;

1.2.33.3. Acesso a base de inteligência global do fabricante para análise online de ameaças;

1.2.34. A interface de administração do sistema deve ter suporte a português do Brasil, devendo ser acessada através de protocolo seguro (HTTPS - HyperText Transfer Protocol Secure) com no mínimo as seguintes funcionalidades:

1.2.34.1. Administração centralizada de todas as regras e filtros integrantes da solução;

1.2.34.2. Status da versão das assinaturas do antivírus em uso;

1.2.34.3. Controle de acesso de usuários, com diferentes privilégios de configuração;

1.2.34.4. Criação de relatórios customizáveis, com gráficos e estatísticas, com suporte a múltiplos domínios;

1.2.34.5. Gerência das áreas de quarentena pelo administrador e possibilidade do usuário gerenciar sua área de quarentena.

1.2.35. A interface de quarentena do usuário deve suportar o idioma português do Brasil;

1.2.36. Permitir efetuar controle profundo dos anexos das mensagens, podendo tomar ações diferenciadas para:

1.2.36.1. Conteúdo do anexo;

1.2.36.2. Mime-Type do anexo;

1.2.36.3. Extensão do anexo;

1.2.36.4. Nome completo do anexo;

1.2.36.5. Nome parcial do anexo;

1.2.36.6. Expressão regular;

1.2.36.7. Tamanho do anexo;

1.2.36.8 Anexos compactados com senha;

1.2.36.9. Quantidade de níveis de compactação no mesmo anexo.

1.3. Proteção Contra Ameaças Avançadas

1.3.1. A solução deverá ser capaz de detectar e bloquear malware novos (ou para o qual não exista assinatura/vacina) / zero-days em anexos e mensagens através da utilização da tecnologia de sandbox em nuvem;

1.3.2. A tecnologia de sandbox em nuvem deverá possuir três níveis de análise: baixo, médio e alto;

1.3.3. A tecnologia de sandbox deverá analisar arquivos macros, no mínimo, JSE, VBE e URL;

1.3.4. A proteção contra Comprometimento de E-mail deverá permitir a criação de uma lista de usuário críticos a serem monitorados.

1.4. Criptografia de E-mail

1.4.1. A solução deverá ser capaz de criptografar e-mails baseado em políticas;

1.4.2. Deve possuir módulo de criptografia do próprio fabricante, já integrado na solução, sem a necessidade de licenciamento adicional, ou seja, já licenciado com a mesma quantidade de caixas postais da solução de proteção de e-mail;

1.4.3. A criptografia deve atuar na saída de e-mails trabalhando de maneira transparente ao usuário final, sem a necessidade de plugins, agentes ou outro tipo de software, com uma interface para o destinatário das mensagens;

1.4.4. A console de gerenciamento do módulo de criptografia deve ser a mesma para toda a solução, não exigindo console de administração adicional;

1.4.5. As políticas deverão conter no mínimo:

1.4.5.1. Endereço de remetente de e-mail, e seu alias;

1.4.5.2. Domínio do remetente,

1.4.5.3. Endereço do Destinatário de e-mail, e seu alias;

1.4.5.4. Domínio do destinatário,

1.4.5.5. Nome ou extensão de anexo,

1.4.5.6. Anexo ou tamanho da mensagem,

1.4.5.7. Número de anexos,

1.4.5.8. Palavras-chave no conteúdo do anexo,

1.4.5.9. Palavras-chave no assunto,

1.4.5.10. Palavras-chave no corpo,

1.4.5.11. Palavras-chave no cabeçalho,

1.4.5.12. Número de destinatário.

1.4.6. Deve possibilitar ao administrador, definir quais mensagens serão criptografadas com base no mínimo em:

1.4.6.1. Assunto;

1.4.6.2. Destinatário;

1.4.6.3. E-mail do Remetente;

1.4.6.4. Nome do Anexo.

1.5. Proteção contra Spam, Vírus, Graymail, Phishing

1.5.1. A solução deverá possuir mecanismo de antivírus para proteção dos e-mails;

1.5.2. A solução deverá possuir mecanismo de reputação de IP;

1.5.3. A solução deverá inspecionar e bloquear anexos com ferramentas de hacking, adware, spyware e programas suspeitos;

1.5.4.A solução deverá permitir e bloquear URL'S não testadas pelo fabricante;

1.5.5. O recurso de reputação de IP deverá permitir adicionar IPs na lista de bloqueados ou aprovados;

1.5.6. A solução deverá permitir a configuração da checagem do TLS;

1.5.7. A configuração do TLS será por domínio com opções de mandatório e oportunista;

1.5.8. A proteção contra BEC (Comprometimento de E-mail) deverá permitir adicionar usuário críticos a fim de detectar ameaças contra eles;

1.5.9. A solução deverá identificar e-mails marketing como redes sociais, fóruns e boletins de informações;

1.5.10. A solução deverá permitir criar exceções para e-mails marketing;

1.5.11. A configuração de spam deverá possuir no mínimo três níveis: baixo, meio e alto;

1.5.12. Proteção contra SPAM

1.5.12.1. Possuir filtro de anti-spam para detecção de spams usando no mínimo as seguintes tecnologias:

a. FingerPrint: Filtro por assinatura de spam;

b. Análise Heurística: Análise completa de toda mensagem contra spam, de acordo com as características da mensagem;

c. Análise de Documentos: Análise de documentos anexados na mensagem (PDF, DOC, DOCX e TXT);

d. Análise de Imagens: Filtragem de spam em imagens;

e. Filtro de URL: Filtragem por URL mal-intencionada contidas no corpo da mensagem, dessa forma combatendo possível e-mail Phishing;

1.5.12.2. Permitir ao administrador definir filtros por URL através de categorias, divididas por assunto, sendo possível definir uma pontuação. Categorias mínimas que devem estar contidas na solução:

a. Conteúdo pornográfico;

b. Abuso infantil;

c. Redes sociais;

d. Racismo e ódio;

e. Pesquisa de empregos;

f. Streaming;

g. Esportes;

h. Notícias;

i. Compras Online.

1.5.12.3. Deve possuir tecnologia capaz de avaliar um link recebido em um e-mail, mesmo que escondido em um e-mail HTML e assim verificar o caminho para o qual este link está apontando, efetuando a verificação se nesta página apontada pelo link há algum formulário de solicitação de senha, usuário e outras ameaças, efetuando o bloqueio da mensagem sem a necessidade de assinatura, tornando assim a proteção mais proativa no combate a phishing;

1.5.12.4. Deve possuir tecnologia capaz de avaliar um link "URL" recebido em um e-mail, mesmo que escondido em um e-mail HTML e assim verificar o caminho para o qual este link está apontando, efetuando a verificação se este link encaminha para um sistema que efetua um redirecionamento automático para download de um arquivos (Tipo Zip, EXE, RAR, etc), na tentativa de enganar o usuário, efetuando o bloqueio da mensagem sem a necessidade de assinatura, tornando assim a proteção mais proativa no combate a phishing;

1.5.12.5. Possuir no mínimo as seguintes tecnologias para prevenção e bloqueio de spam:

a. Recurso de Grey List;

b. Recurso de checagem por SPF (Sender Policy Framework) permitindo a criação de regras individuais e customizadas para usuários ou grupos, permitindo criar ações específicas para “fail” e “soft fail”;

c. Recurso de checagem por DMARC;

d. Recurso de checagem por assinatura DKIM;

e. Recurso de checagem de DNS Reverso;

f. Análise de reputação de IP;

g. Reputação de Mensagens;

h. Filtros de URL;

i. Filtro de anti-phishing;

j. Consulta de RBL´s (real-time blackhole list);

k. Machine Learning.

1.5.12.6. Classificar a reputação de novas origens de spam com tecnologia de classificação dinâmica. O sistema de reputação deve utilizar dados de redes globais de monitoramento de tráfego web e de e-mail, não restringindo ao fluxo de mensagens do ambiente instalado;

1.5.12.7. Possuir a possibilidade de criação de regras personalizadas de filtragem baseadas em:

a. Origens das mensagens;

b. Destino das mensagens;

c. Domínios;

d. Endereços de e-mails;

e. Expressões regulares (dicionário de palavras);

f. Fluxo;

g. Quantidade de mensagens;

h. Tamanho de anexo;

i. Número máximo de destinatários em uma única mensagem;

j. Tipo de arquivos em anexo;

k. Extensões de arquivos em anexo, identificados por Mime-Type;

l. Anexos criptografados;

m. Anexos compactados;

n. Níveis de compactação dos arquivos anexos;

o. Quantidade de anexos na mensagem;

p. Conteúdo HTML no corpo da mensagem.

1.5.12.8. Possibilidade de criar regras para ações a serem tomadas pela ferramenta, quando as mensagens forem consideradas Confiáveis e/ou Spams, permitindo ao administrador configurar nesses casos as seguintes ações:

a. Entregar direto o e-mail;

b. Colocar em quarentena;

c. Remover mensagem;

d. Auditar mensagem;

e. Encaminhar a mensagem;

f. Notificar o destinatário;

g. Adicionar header na mensagem;

h. Transformar HTML em texto simples.

1.5.12.9. Possuir sistema de detecção de ataque de diretórios (DHA – Directory Harvest Attack), capaz de recusar novas conexões SMTP de uma fonte emissora, caso ela tenha enviado, em um período de tempo, mensagens a usuários inválidos/inexistentes no domínio;

1.5.12.10. Deve permitir a criação de regras para aumentar ou diminuir a probabilidade de ser SPAM com base em critérios internos da contratante, permitindo definir no mínimo: país de origem, endereço de domínio, IP do remetente; campo header da mensagem, conteúdo no corpo da mensagem e URL contidas no e-mail;

1.5.12.11. Deve permitir a aplicação de políticas de SPAM diferentes por nome de domínio, destinatário, grupo de destinatários e por destinatário específico, integrado aos sistemas de diretório LDAP e MS Active Directory;

1.5.12.12. Deve ter a capacidade de rejeitar mensagens para destinatários inválidos durante o diálogo SMTP (tratar Non-Delivery Report Attack);

1.5.12.13. Possuir proteção contra bounce e-mail attack através do método “Bounce Address Tag Verification”;

1.5.12.14. Deve permitir a inclusão de múltiplas listas de remetentes bloqueados, permitindo regras de bloqueio se o IP estiver presente nestas listas;

1.5.12.15. Deve permitir que mensagens de Falso Negativo sejam reportadas através da interface gráfica para o laboratório de pesquisa do fabricante ou oferecer um caminho para que mensagens de Falso Negativo sejam reportadas diretamente ao laboratório do fabricante;

1.5.12.16. Deve possuir mecanismo que permita a adição de Cabeçalho de identificação da classificação das mensagens como SPAM, a fim de integrar com sistemas de correio eletrônicos tais como Office 365 - Microsoft Exchange.

1.5.13. Da proteção contra VÍRUS e malwares

1.5.13.1. Deverá ser capaz de filtrar vírus nos dois sentidos de tráfego (entrada e saída de e-mail);

1.5.13.2. Scan de arquivos compactados recursivamente, no mínimo, 5 (cinco) camadas, contemplando no mínimo, os seguintes compactadores: .RAR, .ZIP, .TAR, .ARJ, .CAB, .LHA, .EXE, .LZH, .TGZ, .GZIP, .BZIP, .7Z, .TZH, .TGZ;

1.5.13.3. Deve ter a capacidade de extrair senhas no corpo do e-mail ou no anexo para tentar descriptografar arquivos compactados com senha;

1.5.13.4. Proteção contra Vírus, no mínimo com as tecnologias já licenciadas sem a necessidade de módulo adicional:

a. Dia-zero (zero-day);

b. Vírus outbreak;

c. Hora-zero (Zero-hour);

d. Targeted Attack Protection;

e. APT - advanced persistent threat.

1.6. Rastreamento de e-mail e Auditoria

1.6.1. A solução deverá permitir o rastreamento de mensagens enviadas e recebidas, não será aceito pesquisa via linha de comando;

1.6.2. A solução deverá possuir permitir a consulta de evento com os logs das políticas aplicadas;

1.6.3. O rastreamento de mensagens deverá ser possível através de qualquer dos campos:

1.6.3.1. Data,

1.6.3.2. Direção,

1.6.3.3. IP de origem,

1.6.3.4. Destinatário,

1.6.3.5. Assunto;

1.6.3.6. SHA256, SHA1 ou MD5 ou pelo nome e extensão do anexo

1.6.3.7. Tráfego aceito/tráfego negado;

1.6.3.8. Id da mensagem;

1.6.3.9. Domínio do destinatário;

1.6.3.10. Regra de spam;

1.6.3.11. Regra de DLP;

1.6.3.12. Se a mensagem foi entregue ou não;

1.6.3.13. Pelo tipo da ameaça encontrada.

1.6.4. O rastreamento de mensagens deverá possuir filtros:

1.6.4.1. Última hora;

1.6.4.2. Últimas 24 horas;

1.6.4.3. Últimos 7 dias;

1.6.4.4. Últimos 14 dias;

1.6.4.5. Últimos 30 dias;

1.6.4.6. Customização de período;

1.6.4.7. Por e-mail real ou por alias;

1.6.5. O log de política deverá possuir os seguintes campos: data, origem, destinatário, assunto, nome da regra, tipo de ameaça e id da mensagem;

1.6.6. A solução deverá possuir logs das atividades realizadas no console;

1.6.7. A solução deverá permitir realizar o rastreamento dos usuários que clicaram em URL'S baseado na política de click de URL;

1.6.8. Deve apresentar ainda as seguintes características de rastreamento de mensagens:

1.6.8.1. Rastreamento completo de mensagens aceitas, retidas e rejeitadas, desde o recebimento da mensagem pelo IP cliente até a entrega para o IP destino, usando como filtro o assunto, o remetente, o destinatário, regra de bloqueio, data, status, hora de entrega da mensagem, permitindo a concatenação dos filtros através dos operadores lógicos "e";

1.6.8.2. O rastreamento deve ser a partir de uma única interface de gerenciamento, não sendo aceito pesquisa via linha de comando;

1.6.8.3. O rastreamento deverá ter a opção de ser efetuado de todos os pontos de filtragem, sem a obrigatoriedade de separação de um único ponto de filtragem por vez;

1.6.8.4. Deve apresentar como resultado as seguintes informações:

a. Remetente da mensagem;

b. Destinatários da mensagem;

c. Servidor de origem;

d. Se foi armazenada em quarentena;

e. Se continha vírus;

f. A regra que atuou;

g. O servidor de origem;

h. O tamanho da mensagem;

i. Se foi entregue ou não;

1.6.8.5. No caso de a mensagem ter sido entregue, deve ser possível a apresentação do log de entrega da mesma e para qual IP entregue;

1.6.8.6. Se o e-mail tiver sido bloqueado por ser considerado spam ou possível spam, o log deve apresentar os filtros aplicados e explicação do que representa o filtro aplicado (para facilidade do entendimento do administrador);

1.6.8.7. Rastrear e-mails a partir de uma determinada ameaça;

1.6.8.8. Apresentar na interface gráfica as fontes de ataque e, através delas, apresentar quais e-mails foram recebidos, originários dessa fonte de ataque.

1.7. Notificações e Relatórios

1.7.1. A solução deverá suportar via notificação via e-mail, atendendo aos seguintes parâmetros:

1.7.1.1. A solução deverá permitir ao administrador agendar o envio do resumo das mensagens na quarentena individual do usuário (digest) em períodos de tempo pré-configuráveis por horário e dia, possibilitando ações do usuário diretamente através dos comandos definidos neste digest, dispensando a instalação de agentes e acesso a quarentena individual do usuário;

1.7.1.2. Desejável que grupos diferentes de usuários devem poder receber a notificação em horários diferentes;

1.7.1.3. O digest deve ser enviado em Língua portuguesa do Brasil, mas com a possibilidade de customização do texto, para todos os usuários ou para um determinado grupo de usuários;

1.7.1.4. Deve ser possível a customização do digest com as seguintes características alteráveis:

a. E-mail de origem;

b. Título/Assunto do e-mail;

c. Mensagem do digest, com possibilidade de inclusão de imagens e links, bem como mudança de fonte, alinhamento e cor;

d. Logomarca do digest;

1.7.1.5. O digest deve permitir ao usuário final tomar no mínimo as ações de:

a. Liberar uma mensagem bloqueada;

b. Bloquear o remetente da mensagem (blacklist), para que as futuras mensagens dele já sejam barradas;

c. Marcar o remetente como confiável (whitelist), para que as futuras mensagens do mesmo não sejam pontuadas como SPAM;

d. Reportar o bloqueio indevido;

e. Acessar sua área de quarentena;

1.7.1.6. Deve permitir que o administrador escolha qual quarentena a ser incluída no digest do usuário final, por exemplo incluir no digest os e-mails quarentenados que foram considerados conteúdos maliciosos por comportamento ou aprendizado de máquina;

1.7.1.7. A solução deverá permitir ao administrador selecionar quais ações serão liberadas para o usuário final selecionar, no mínimo:

a. Liberar e-mail;

1.7.1.8. Incluir o remetente do e-mail em blacklist individual (do próprio usuário);

1.7.1.9. Incluir o remetente do e-mail em whitelist individual (do próprio usuário);

1.7.1.10. Visualizar o e-mail;

1.7.2. A solução deverá possuir modelos de notificação pré-definidas para violação de políticas;

1.7.3. A solução deverá suportar notificar quando o e-mail possuir um anexo compactado;

1.7.4. A solução deverá notificar quando o tamanho da mensagem for excedido;

1.7.5. A solução deverá notificar quando uma regra for desencadeada;

1.7.6. A solução deverá notificar quando houver uma configuração de violação de segurança;

1.7.7. A solução deverá notificar quando um vírus, SPAM etc., for detectado;

1.7.8. A solução deverá possuir relatórios nativos com informações sobre as ameaças detectadas;

1.8. Dos relatórios:

1.9. Deve permitir a geração de relatórios de forma centralizada através de interface web do gateway de e-mail ou do módulo de inspeção de e-mails entre caixas de correio;

1.10. Deve ser capaz de gerar relatórios gráficos e agendar o envio dos mesmos a usuários específicos via e-mail;

1.11. Deve ser capaz de gerar relatórios por data ou por um intervalo de tempo específico;

1.12. Deve ser possível configurar um período para a retenção (podendo ser em até 90 dias) dos dados utilizados para geração dos relatórios;

1.13. Capacidade de criar relatórios contendo no mínimo as seguintes informações:

1.13.1. Sumário de mensagens;

1.13.2. Quantidade de mensagens processadas;

1.13.3. Relatório de Volume de Mensagens por Data;

1.13.4. Principais origens de spam por domínio, endereço de e-mail;

1.13.5. Principais destinos de spam por domínio, endereço de e-mail;

1.13.6. Principais origens de vírus;

1.13.7. Principais fontes de ataque;

1.13.8. Conexões completadas X bloqueadas;

1.13.9. Relatório de tráfego;

1.13.10. Principais destinatários de Spam;

1.13.11. Principais destinatários de e-mail;

1.13.12. Top Ataques por fraude de e-mail / tentativa de spoof.

1.13.13. Permitir filtros de relatórios com definição de origem e destinos específico;

1.13.14. Possuir relatórios estatísticos de conexões, ameaças, quarentena e SPAM;

1.14. Deve apresentar estatísticas e monitoramento em tempo real (online) de e-mails com base em gráficos;

1.15. Os relatórios, no mínimo, devem poder ser filtrados por:

1.15.1. Período de tempo;

1.15.2. Ponto de Filtragem que o e-mail passou;

1.15.3. De;

1.15.4. Para;

1.15.5. Qual a classificação que a mensagem atingiu, dentre eles no mínimo:

1.15.5.1. DLP;

1.15.5.2. Provável SPAM;

1.15.5.3. SPAM;

1.15.5.4. Vírus;

1.15.5.5. Conteúdo Bloqueado;

1.15.5.6. Whitelist;

1.15.5.7. Blacklist;

1.15.5.8. Tamanho Excedido;

1.15.5.9. Phishing.

1.15.6. Relatório para um único usuário ou Domínio.

1.16. A solução deverá permitir a integração com Syslog e soluções de Siem, permitir exportar para arquivos tipo CSV;

2. Prevenção contra Vazamento de Dados

2.1. A solução deverá possuir permitir o recurso de prevenção contra vazamento de dados;

2.2. A solução deverá possuir uma base com, no mínimo, 50 modelos para criação de regras;

2.3. A solução deverá permitir a customização de modelos para a LGPD;

2.4. A solução deverá possuir permitir criar regras baseados em extensões de arquivos, expressões regulares e atributos de arquivos;

3. Quarentena de E-mails

3.1. A solução deverá permitir o gerenciamento da quarentena para múltiplos domínios;

3.2. A solução deverá permitir a utilização de quarentena por usuário, possibilitando que cada usuário cadastrado em um controlador de diretório LDAP ou Microsoft Active Directory, que esteja integrado com a solução, administre suas próprias mensagens categorizadas como spam;

3.3. A solução deverá permitir a customização da notificação de quarentena pela menos semanal, uma vez ou mais vezes durante o dia;

3.4. A notificação de quarentena deverá permitir a customização;

3.5. A notificação de quarentena deverá ser no mínimo em inglês e/ou português no e-mail com o resumo da quarentena;

3.6. A solução deverá fornecer a opção de adicionar o e-mail em uma lista de rementes aprovados;

3.7. Permitir ao administrador da solução executar pesquisa nas áreas de quarentena de todos os usuários através de interface web segura (HTTPS), acessando o próprio sistema de gerenciamento, sem necessidade de nenhum hardware adicional;

3.8. Deve possibilitar a gestão de quarentena pelos administrados de forma que eles possam visualizar a razão de um determinado bloqueio, remetente, destinatário, data, assunto, IP do host destinatário, a mensagem original, tamanho da mensagem original e permitindo no mínimo as ações liberar e/ou excluir;

3.9. Caso uma mensagem seja bloqueada ou rejeitada, a solução deverá informar também a razão do bloqueio e quais regra foram ativadas;

3.10. A interface deve permitir identificar quais Regras do Modulo de AntiSpam foram ativadas, a fim de permitir ao administrador a elaboração de regras granulares;

3.11. A solução deve suportar a criação de áreas de quarentena personalizadas para usuários específicos, e:

3.11.1. Deve permitir também que todas as áreas de quarentenas sejam armazenadas de forma criptografadas.

3.11.2. Deve permitir que o tempo de armazenamento da quarentena seja individual por cada área de quarentena de usuário;

3.11.3. Deve permitir a visualização do resumo de todas as áreas de quarentena e volume de mensagens;

3.12. O sistema de quarentena de e-mails deve criptografar automaticamente as mensagens armazenadas, evitando o acesso não autorizado aos arquivos e ao conteúdo dos e-mails armazenados em quarentena, assim aumentando a confiabilidade e segurança da solução;

3.13. O tempo de armazenamento da quarentena deve ser individual por área de quarentena, devendo também permitir armazenamento por pelo menos 30 dias;

3.14. Possibilitar ao administrador selecionar o rotacionamento das mensagens em quarentena por tamanho da quarentena, sendo que ao ultrapassar o limite deste tamanho, o sistema automaticamente começará a apagar os e-mails quarentenados mais antigos;

3.15. O administrador ao criar uma quarentena customizada, deverá ter a capacidade de selecionar quais usuários poderão ter acesso a ela;

4. Modulo de inspeção de e-mails entre caixas de correio

4.1. Deve ter a capacidade de analisar arquivos e URLs em sandbox para identificação de ameaças desconhecidas (sem assinatura);

4.2. Deve utilizar mecanismos de proteção que contemplem, pelo menos, malwares conhecidos por assinatura, malwares desconhecidos por Machine Learning, bloqueio de conteúdo (por tipo de arquivo, por exemplo), reputação de URLs;

4.3. A solução deve permitir compartilhamento de informações através de SIEM via Syslog ou através da gerência centralizada;

4.4. A solução deve prover relatórios que contemplem, pelo menos, riscos de segurança (ameaças), ransomware, arquivos analisados em sandbox, auditoria;

4.5. Os relatórios devem ser exportáveis para, pelo menos, PDF;

4.6. Os relatórios devem ser enviados por email, mediante configuração do administrador;

4.7. Aplicar proteções anti-malware, verificação de URL's maliciosas para a proteção dos serviços.

4.8. A verificação Anti-malware deverá permitir e customização das ações a serem tomadas, por exemplo: quarentenar, deletar e passar.

4.9. Aplicar proteções contra Comprometimento de E-mail utilizando análise de escrita.

4.10. Realizar integração nuvem-a-nuvem, através de API ou conectores de fluxo de e-mail da Microsoft , realizando a análise de malware em sandbox.

4.11. Monitorar em tempo real para bloquear, colocar em quarentena ou permitir fazer relatórios do estado atual;

4.12. Empregar detecção de malware por meio de sandbox sem assinaturas, para diminuir seu risco de violação.

4.13. Monitorar o comportamento real de arquivos suspeitos em ambientes sandbox virtuais, usando múltiplas versões de sistemas operacionais e aplicações;

4.14. As políticas deverão possuir a capacidade de serem realizadas por usuário ou grupo.

4.15. Possuir um dashboard com as principais ameaças detectadas, a exemplo dos tipos Ransomware, Phishing, Comprometimento de E-mail.

4.16. A solução deverá ser capaz de implementar políticas com base no filtro de conteúdo das mensagens.

4.17. A solução deverá compartilhar objetos suspeitos previamente analisados em Sandbox do próprio fabricante.

4.18. A solução deverá entregar o e-mail somente após concluir a análise do objeto suspeito. Este processo deverá ocorrer em média de 5 minutos;

4.19. Os alertas enviados deverão permitir a customização tanto para o usuário quanto para o administrator.

4.20. Deverá possui a funcionalidade de verificação de SPAM com níveis de detecções diferentes.

4.21. As ações realizadas pelo antispam deverão possuir as seguintes opções: quarentena, adicionar uma tag no assunto, deletar ou mover para a pasta de lixo.

4.22. Deverá permitir o administrador adicionar ou bloquear um endereço na lista de remetentes.

5. Do Gerenciamento

5.1. O acesso à interface de administração deve possuir diferentes níveis de permissões, de forma granular, permitindo que sejam configurados perfis diferentes, por endereços de e-mail e domínio permitidos;

5.2. O sistema deve permitir a customização para, pelo menos as seguintes funções:

5.2.1. Administrador: Com acesso total às configurações da solução;

5.2.2. Administrador: Com acesso total às configurações da solução sem acesso à leitura dos e-mails armazenados tanto na quarentena como mensagens auditadas;

5.2.3. Auditor: Com acesso a visualização dos e-mails armazenados para auditoria;

5.2.4. Operador: Com acesso à administração da quarentena e gerenciamento da “Black e White List”;

5.2.5. Usuário: Possui a capacidade de administrar sua “Black e White List”, individualmente, bem como sua área de quarentena individual.

6. Das Funcionalidades para o Usuário Final

6.1. Possuir interface web de administração segura HTTPS para que cada usuário final possa administrar suas opções pessoais e sua quarentena, sem que estas opções interfiram na filtragem dos demais usuários;

6.2. A interface do usuário final deve estar no idioma configurado pelo administrador, sendo no mínimo os seguintes idiomas:

6.2.1. Português do Brasil.

6.2.2. Inglês.

6.3. O usuário final deve ser capaz de incluir e remover endereços em sua lista pessoal de bloqueio ou de liberação de e-mails;

6.4. O usuário final deve ser capaz de visualizar as mensagens bloqueadas e liberá-las, a seu critério, desde que as mesmas sejam consideradas somente como “possível spam” ou “spam”;

6.5. O usuário deverá ser capaz de selecionar qual o idioma utilizado na sua interface administrativa, sendo no mínimo os seguintes idiomas:

6.5.1. Português do Brasil;

6.5.2. Inglês;

6.5.3. Espanhol;

7. Dos Usuários e Grupos

7.1. Possuir integração com serviço de diretórios LDAP, Microsoft Active Directory para obtenção de informações de usuários cadastrados para validação de destinatário e configuração de políticas, bem como impedir ataques de dicionário (“Directory Harvest Attack”);

7.2. Permitir criação de conectores para múltiplos serviços de diretório, por exemplo conector para servidor LDAP e outro conector para Microsoft Active Directory;

7.3. Permitir a utilização de mais de um servidor de LDAP ou Microsoft Active Directory ao mesmo tempo. Caso ocorra indisponibilidade do servidor primário a autenticação dos usuários deverá ocorrer normalmente no outro servidor configurado;

7.4. Integração nativa com o Microsoft Exchange;

7.5. Possibilitar a customização de regras e políticas por usuários ou grupos;

7.6. A solução deverá permitir a configuração do intervalo de sincronismo com o serviço de diretório;

7.7. Permitir atrelar grupos a regras específicas de rotas, por exemplo: Não aplicar determinada regra do módulo de antivírus para os e-mails que vierem de um determinado domínio, sendo que esta regra somente será aplicada a um grupo específico de usuários.

8. Proteção contra ataques direcionados

8.1. A solução deve ser capaz de bloquear ataques de negação de serviço (Denial of Service);

8.2. Ser uma solução MTA (Mail Transfer Agent) completa suportando o protocolo SMTP, e com suporte a envio e recebimento de e-mails criptografados utilizando o protocolo TLS a partir da versão 1.1, permitindo configurar domínios onde o TLS é mandatório;

8.3. Deve ser capaz de efetuar a filtragem do tráfego de correio eletrônico bloqueando a entrada e saída de:

8.3.1. Vírus;

8.3.2. Spyware;

8.3.3. Worms;

8.3.4. Trojans;

8.3.5. Spam;

8.3.6. Phishing;

8.3.7.E-mail Marketing, ou qualquer outra forma de ameaça virtual.

8.4. Deve possuir controle total da comunicação permitindo restringir:

8.4.1. IP reverso mal configurado;

8.4.2. Domínios inexistentes;

8.4.3. Permitir identificar e bloquear e-mails vindos de domínios recentemente cadastrados.

8.5. Deve permitir ao administrador criar filtros e assinaturas, bem como realizar atualização automática das mesmas, em frequência de consulta configurada pelo administrador.

8.6. Permitir criação de políticas customizadas para tratamento de spam, vírus e filtragem de conteúdo, de acordo com o destinatário da mensagem;

8.7. Permitir configurar ações diferenciadas sobre as mensagens suspeitas, incluindo:

8.7.1. Aceitar;

8.7.2. Colocar em quarentena;

8.7.3. Inserir tag personalizada no assunto;

8.7.4. Marcar o cabeçalho.

8.8.A solução deve ser capaz de tomar as seguintes ações sobre as mensagens:

8.8.1. Alterar o assunto da mensagem;

8.8.2. Adicionar cabeçalhos para rastreamento;

8.8.3. Descartar a mensagem;

8.8.4. Colocar em uma determinada área de quarentena definida pelo administrador.

8.9. Deve permitir a criação de regras baseadas por país;

8.10. Possuir a capacidade de criar filtros personalizados usando expressões regulares;

8.11. Permitir criação de listas negras e listas brancas, com opção por domínio, subdomínio, endereço de e-mail e endereço IP;

8.12. Deve prover um mecanismo que impeça a sua utilização como retransmissor de mensagens originadas externamente (relay);

8.13. Capacidade de limitar o número máximo de mensagens enviadas por remetente a cada hora, com opção de bloqueio automático do remetente, caso esse limite seja excedido;

8.14. Permite criar regras customizáveis contra spammers, possibilitando um controle avançado em todo conteúdo do e-mail efetuando buscas por Expressões Regulares presentes em todo conteúdo do e-mail (SMTP HEADER, BODY, URL, ANEXOS), sendo possível criar regras compostas utilizando os operadores lógicos “E” e “OU”;

8.15. O fabricante da solução deve possuir consulta de reputação de IP de remetentes de e-mail. Esta consulta deve retornar os dados do remetente, com informações referentes à:

8.15.1. IP reverso e localização;

8.15.2. Registro em blacklists mundiais;

8.15.3. Configuração de serviço de notificação de envio e autenticidade de mensagens de mensagens como SPF e DKIM.

8.16. Capacidade de efetuar consultas externas ou internas na própria console da solução, para análise de endereço IP do remetente quanto a sua reputação, bem como verificação de spams e phishings recebidos e outros tipos de ameaças;

8.17. Deve ser capaz de realizar reverse DNS LookUp (rDNS), para validação de fontes de e-mail;

8.18. Deve possuir suporte ao bloqueio de conexões de e-mails nocivos durante o diálogo SMTP, em especial baseado em lista local de bloqueio de conexão por:

8.18.1. IP;

8.18.2. E-mail;

8.18.3. Domínio;

8.19. Deve ter capacidade de proteção a spoofing de e-mail (tanto Spoofing de e-mails na entrada – quando o hacker utiliza o domínio do órgão como remetente, como Spoofing de e-mails na saída – quando tem algum e-mail de saída que não esteja com o domínio do órgão como remetente);

8.20. Possuir capacidade de criar cotas de envio e recebimento de e-mails em um prazo determinado de tempo, limitando o fluxo e prevenindo ataque do tipo DOS ou distribuição de spam através de um computador infectado na rede interna;

8.21. Deve ser capaz de limitar o fluxo de mensagens automaticamente, de acordo com o volume de mensagens indevidas recebidas de um determinado IP de origem;

8.22. Possuir funcionalidade de verificação de DMARC (Domain-based Message Authentication Reporting & Conformance);

8.23. Deve possuir apresentação de ameaças detectadas em tempo real. Nesse sistema de detecção de ameaças em tempo real, deve ser possível identificar:

8.23.1. Fontes de ataques;

8.23.2. Ameaças encontradas.

8.24. Deverá prover proteção contra ataques dirigidos tais como:

8.24.1. Spear-phishing;

8.24.2. Ataques Zero-Day;

8.24.3. Ameaças avançadas persistentes (APTs).

8.25. Deve possuir técnica para construção de modelos estatísticos com Big Data;

8.26. Deve possuir no mínimo 3 (três) camadas de proteção sendo elas:

8.26.1. Verificação da lista de códigos maliciosos: Verificação de campanhas de e-mails emergentes e conhecimento de novos sites maliciosos;

8.26.2. Análise Estática (Análise de código): Verificação de comportamento suspeito, scripts escondidos, partes de códigos maliciosos e redirecionamento a outros sites maliciosos;

8.26.3. Análise Dinâmica: Utilização de “Sandbox” para simular a máquina de um usuário real e observar as alterações efetuadas no sistema.

8.27. Possuir, dentro da solução, um dashboard do módulo de Segurança contra-ataques dirigidos;

8.28. O sistema de proteção contra-ataques dirigidos deve executar no mínimo 3 (três) etapas:

8.28.1. Detecção - A análise de e-mail deve verificar variáveis em tempo real incluindo as propriedades da mensagem, bem como, o histórico de e-mail do destinatário para identificar anomalias que indiquem uma ameaça potencial;

8.28.2. Proteção - Deve assegurar que links para URLs suspeitas são dinamicamente reescritas antes que o e-mail seja entregue ao destinatário. Cada vez que um usuário clica em um destes links esteja ele na empresa ou em um local remoto o serviço verifica se o destino é seguro;

8.28.3. Ação - Deve demonstrar aos administradores e gestores de segurança em tempo real e de forma interativa uma visão dos ataques sofridos e das ameaças que possam sofrer, passando para usuários específicos, dispondo de ferramentas para ajudar a remediar danos, tudo baseado em um painel de controle online.

8.29. Não será aceita solução baseada apenas em reputação de URL;

8.30. A solução deve conter engine para detecção de Anomalias, não podendo se limitar a análise com definições baseadas em ataques já conhecidos;

8.31. Deve ser possível habilitar ou desabilitar a proteção URL baseada em rotas especificas configuradas no mínimo pelas seguintes condições:

8.31.1. E-mail do Destinatário;

8.31.2. E-mail do Remetente;

8.31.3. Domínio de Origem;

8.31.4. Domínio de Destino;

8.31.5. IP/Rede;

8.31.6. Range de IP;

8.31.7. Expressão Regular;

8.31.8. Usuários;

8.31.9. Listas de distribuição;

8.31.10. Grupo de LDAP.

8.32. A proteção de URL deverá reescrever os links do e-mail e a cada clique o sistema deverá analisar a URL e somente depois de passar por todos os testes, sendo constatado que não é malicioso, deve redirecionar para a URL original. Se após a análise for constatado site malicioso, o sistema deverá exibir mensagens de alerta e o site deverá ser bloqueado para acesso;

8.33. O sistema deverá ser capaz de varrer anexos, com no mínimo, tipos PDF, arquivos em Flash para payloads maliciosos e Microsoft Office;

8.34. Ao detectar arquivos maliciosos, deverá ser capaz de configurar regras para descartar e salvar uma cópia na quarentena;

8.35. Deve possuir tecnologia SandBox em nuvem do próprio fabricante no Brasil, desde que esteja em conformidade com todas as regras da legislação vigente brasileira (Lei Geral de Proteção de Dados Pessoais);

8.36. Deverá ser capaz de efetuar a verificação da reputação de anexos e caso a reputação do anexo não conste no banco de dados, a solução deverá ter a opção de enviar automaticamente o anexo para a nuvem do fabricante para análise em tempo real em sistema de SandBox do próprio fabricante, caso o administrador opte por este serviço. Este sistema de SandBox deve conter tecnologia de detecção usando "Análise Comportamental" do arquivo identificando assim malwares e variantes sem a necessidade de assinaturas;

8.37. A proteção URL deverá acompanhar o destinatário na URL reescrita. Quando uma mensagem for dirigida a vários destinatários, o envelope será dividido de modo que existam apenas um receptor associado com uma URL reescrita para permitir que administradores possam controlar quais usuários clicaram na URL reescrita e os usuários que ignoraram através do Dashboard;

8.38. A proteção URL deverá reescrever links para os protocolos HTTP, HTTPS, FTP;

8.39. A solução deverá permitir que o administrador configure o sistema de proteção URL para que reescreva todas as mensagens que contiverem URL e envie ao sandbox para testes garantindo um alto nível de segurança;

8.40. A solução deverá prover lista de exceções de URL para que não sejam reescritas;

8.41. O Dashboard deverá exibir o número de cliques em cada ameaça;

8.42. O Dashboard deverá exibir qual usuário clicou na URL detectada como ameaça;

8.43. O Dashboard deverá exibir informações atualizadas sobre as ameaças detectadas, deverá exibir a classificação da mensagem e deverá exibir status atualizado e detalhado sobre as ameaça no mínimo com as seguintes informações:

8.43.1. Clicado – Número de vezes que uma URL reescrita foi clicada por um usuário, inclusive se a mensagem for encaminhada para outro usuário e também for clicada;

8.43.2. Bloqueado - Número de vezes que o modulo de Proteção URL impediu o usuário de acessar o site malicioso;

8.43.3. Permitida – Número de vezes que o modulo de proteção URL permitiu ao usuário acessar o site original da URL reescrita e que não foi detectada como maliciosa.

8.44. Deve possuir módulo de CDR "Content Disarm and Reconstruction", que quando ativado irá remover conteúdos possivelmente perigosos, em no mínimo para os seguintes tipos:

8.44.1. JavaScript;

8.44.2. Links;

8.44.3. Executáveis;

8.44.4. VB Script.

8.45. De dentro de documentos, em no mínimo para os seguintes tipos:

8.45.1. pdf;

8.45.2. doc;

8.45.3. docx;

8.45.4. ppt;

8.45.5. pptx;

8.45.6. xls;

8.45.7. xlsx.

8.46. Deve possuir capacidade de ignorar reescrita de algumas URL's e não envio de arquivos para análise no SandBox do fabricante;

8.47. O SandBox do fabricante deve ter a capacidade de analisar arquivos, mesmo que estejam inseridos em arquivos compactados, do tipo:

8.47.1. .swf;

8.47.2. .pdf;

8.47.3. .doc;

8.47.4. .xls;

8.47.5. .xlsx;

8.47.6. .ppt;

8.47.7. .ppt;

8.47.8. .pptx;

8.47.9. .rtf.

8.48. Deve ter a opção de não fazer reescrita de URL's em casos de mensagens oriundas de determinados domínios,

8.49. A solução deverá ter a capacidade de criar exceções para a reescrita de URLs oriundas de determinados domínios, desabilitando essa funcionalidade para domínios previamente configurados.

8.50. Possibilidade do administrador de incluir URL's, arquivos e IP's em uma lista de bloqueio (Blacklist) no sistema de detecção;

8.51. Possibilidade do administrador de incluir URL's, arquivos e IP's em uma lista segura (Whitelist) no sistema de detecção.

9. Prevenção a roubo de informação (DLP) e Compliance

9.1. Deve possuir módulo DLP (Data Loss Prevention) do próprio fabricante, já integrado na solução, sem a necessidade de licenciamento adicional, ou seja, já licenciado com a mesma quantidade de caixas postais da solução de proteção de e-mail;

9.2. O módulo de DLP deve analisar todo conteúdo da mensagem a fim garantir a confiabilidade das mensagens que saem da empresa, permitindo ao administrador configurar diversas ações a fim de restringir, controlar ou auditar as mensagens e informações sensíveis da empresa;

9.3. Deve permitir criar regras de compliance "Auditoria/Aderência" através de filtros avançados de análise da mensagem, permitindo identificar através de Dicionários (Conjunto de Palavras e Expressões Regulares) personalizados pelo administrador ou já existentes na ferramenta, dentre eles:

9.3.1. Identificação de CPF;

9.3.2. Número de cartão de crédito;

9.3.3. CNPJ.

9.4. As regras de conformidade podem ser criadas utilizando os termos dos dicionários definidos e que estejam nos seguintes campos da mensagem, podendo ser definido o número de ocorrências mínimas para execução da regra:

9.4.1. Cabeçalho;

9.4.2. URL (contidas no e-mail);

9.4.3. Corpo do e-mail;

9.4.4. Anexos e documentos no mínimo: .DOC, .DOCX, .XLS, .XLSX, .PDF, .PPT, .PPTX e .TXT.

9.5. Permitir ao administrador criar regras de compliance para arquivos criptografados, possibilitando ao administrador configurar a ação a ser tomada quando um anexo criptografado é identificado. A ferramenta deve ter no mínimo três algoritmos de detecção: Mecanismo Heurístico, Myme-Type e Extensão;

9.6. Todos os itens do DLP devem permitir configurações através de regras que permitam ao administrador definir, no mínimo, as seguintes ações:

9.6.1. Entregar a mensagem;

9.6.2. Não entregar a mensagem;

9.6.3. Armazenar a mensagem para auditoria;

9.6.4. Notificar remetente e destinatário da mensagem;

9.6.5. Encaminhar a mensagem para outro destinatário.

9.7. Todos os itens do DLP devem permitir configurações que permitam ao administrador criar regras complexas através de operadores lógicos "E" e "OU";

9.8. Deve permitir ao administrador gerar notificação (se assim desejar) ao remetente do e-mail, indicando que o e-mail enviado não condiz com as normas da empresa. Essa notificação poderá ser customizada de acordo com a necessidade do administrador;

10. Do Sistema de Proteção a Fraudes de E-mail

10.1. Deve possuir capacidade de detecção de Spoofing de e-mails externos, isto é, ter a capacidade de comparar o domínio do cabeçalho do e-mail (Header do E-mail/Envelope SMTP), com o domínio apresentado como remetente para o usuário final (Cabeçalho From) e indicar o que deve ser feito se forem diferentes:

10.1.1. Pontuar;

10.1.2. Ignorar;

10.1.3. Bloquear.

10.2. O sistema deve possuir a opção de configurar regras para detectar e-mails que estejam utilizando ataques do tipo Look-A-Like Domain, isto é, detectar e-mails com domínios similares aos domínios utilizados pelo órgão;

10.3. Deve possuir sistema de detecção de e-mails oriundos de servidores de e-mails gratuitos tais como Google, Yahoo, Hotmail, etc., para serem usados em regras personalizadas de filtragem;

10.4. Nativamente deve possuir sistema de detecção de e-mails externos (e-mails de entrada) que tentem utilizar o domínio da própria empresa como remetente, sem necessidade de criação de regra específica para este tipo de fraude.

11. Da Migração da solução Atual

11.1. A empresa vencedora será responsável por realizar a migração de todas as regras e filtros configurados na atual solução em uso pelo Ministério Público.

12. Confidencialidade

12.1. A solução deverá tratar todas as mensagens de maneira automatizada e sem intervenção humana.

12.2. As mensagens analisadas pela solução não serão armazenadas, a não ser nos seguintes cenários:

12.2.1. No caso de falha do serviço de MTA do Ministério Público (neste caso o armazenamento esperado deverá ser de no mínimo 10 dias);

12.3. No caso da implantação de política de retenção de mensagens por meio de quarentena (neste caso as mensagens armazenadas deverão estar disponíveis por pelo menos 90 dias).

APENSO II

TERMO DE COMPROMISSO, SIGILO E CONFIDENCIALIDADE

Os abaixo-assinados, de um lado o **MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA**, CNPJ nº 04.142.491/0001-66, situado na cidade de Salvador, a 5ª Avenida, 750 – Centro Administrativo da Bahia, doravante denominado **CONTRATANTE**, e de outro lado **EMPRESA HSC DESENVOLVIMENTO E SERVIÇOS EM TECNOLOGIA DA INFORMAÇÃO LTDA**, CNPJ nº 13.103.980/0001-08, situada na cidade de Porta **Alegre/RS, à Rua General João Manoel, 50, 5° andar, sala 502, Centro Histórico**, doravante denominada **CONTRATADA**, tem entre si justa e acertada, a celebração do presente **TERMO DE COMPROMISSO, SIGILO E CONFIDENCIALIDADE**, através do qual a **CONTRATADA** aceita não divulgar sem autorização prévia e formal segredos e informações sensíveis de propriedade do **CONTRATANTE** e se compromete a praticar procedimentos de segurança da informação, em conformidade com as seguintes cláusulas e condições:

CLÁUSULA PRIMEIRA – A **CONTRATADA** reconhece que, em razão das suas atividades profissionais, estabelece contato com informações confidenciais, que devem ser tratadas, indispensavelmente, com o sigilo necessário, não podendo ser divulgadas a terceiros não autorizados, inclusive aos próprios Colaboradores da **CONTRATADA**, sem a expressa e escrita autorização do **CONTRATANTE**.

CLÁUSULA SEGUNDA - As informações, exemplificadas abaixo, devem receber o tratamento de confidencialidade adequado, de acordo com o seu nível de classificação.

1. Programas de computador, suas listagens, documentação, artefatos diversos, código fonte e código objeto;

2. Toda a informação relacionada a programas existentes ou em fase de desenvolvimento no âmbito do **CONTRATANTE**, inclusive fluxogramas, estatísticas, especificações, avaliações, resultados de testes, arquivos de dados, artefatos diversos e versões "beta" de quaisquer programas;

3. Documentos, informações e dados armazenados de atuação consultiva e contenciosa, de estratégias ou demais dados e/ou informações de caráter sigiloso ou restrito a;

4. Metodologia, projetos e serviços utilizados;

5. Números e valores financeiros;

6. Demais informações trafegadas no ambiente de rede da **CONTRATANTE**, como arquivos e e-mails.

CLÁUSULA TERCEIRA – A **CONTRATADA** reconhece que, além da lista acima, outras hipóteses de confidencialidade que já existam, ou que venham a surgir no futuro, devem ser mantidas sob sigilo. Em caso de dúvida acerca da confidencialidade de determinada informação, a **CONTRATADA** deve tratar a mesma como se sigilosa fosse até que seja autorizado, formalmente, a tratá-la de forma diferente pelo **CONTRATANTE**.

CLÁUSULA QUARTA – A **CONTRATADA** reconhece que, reconhece que, no seu desligamento definitivo do contrato, deverá entregar ao **CONTRATANTE** todo e qualquer material de propriedade desta, inclusive notas pessoais envolvendo matérias sigilosas relacionadas com a atividade, registros de documentos de qualquer natureza que tenham sido usados, criados ou estado sob seu controle. A **CONTRATADA** também assume o compromisso de não utilizar qualquer informação adquirida quando de suas atividades para o **CONTRATANTE**.

CLÁUSULA QUINTA – A **CONTRATADA** deve assegurar que todos os seus colaboradores guardarão sigilo sobre as informações que porventura tiverem acesso, mediante o ciente de seus colaboradores em Termo próprio a ser firmado entre a **CONTRATADA** e seus colaboradores, e que os mesmos comprometer-se-ão a informar, imediatamente, ao seu superior hierárquico, qualquer violação das regras de sigilo, por parte dele ou de qualquer pessoa, inclusive nos casos de violação não intencional.

§1º A coleta dos Termos de Sigilo de seus colaboradores não exime a **CONTRATADA** das penalidades por violação das regras por parte de seus contratados.

§2º A **CONTRATADA** deverá fornecer cópia de todos os termos firmados com seus colaboradores quando do início dos trabalhos.

§3º Sempre que um colaborador for admitido, a **CONTRATADA** deverá fornecer cópia do respectivo termo de sigilo por aquele firmado, no prazo de 2 (dois) dias após a contratação.

CLÁUSULA SEXTA - A **CONTRATADA** deverá seguir a Política de Segurança da Informação definida pelo **CONTRATANTE**.

CLÁUSULA SÉTIMA - O não cumprimento de quaisquer das cláusulas deste Termo implicará em responsabilização administrativa, civil e criminal, de acordo com a legislação vigente.

Em,_____de _____de 2021.

Ministério Público do Estado da Bahia
Frederico Welington Silveira Soares
Superintendente de Gestão Administrativa

Empresa Hsc Desenvolvimento e Serviços em Tecnologia da Informação Ltda
Romulo Giordani Boschetti
Representante legal

Documento assinado eletronicamente por **ROMULO GIORDANI BOSCHETTI** em 08/01/2021, às 17:08, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Frederico Welington Silveira Soares** em 08/01/2021, às 17:50, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.sistemas.mpba.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0067797** e o código CRC **A76FE8BD**.

MINISTÉRIO PÚBLICO
DO ESTADO DA BAHIA

PORTARIA

PORTARIA Nº 002/2021

O **SUPERINTENDENTE DE GESTÃO ADMINISTRATIVA DO MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA**, no uso de suas atribuições legais,

RESOLVE

Designar os servidores Iaçanã Lima de Jesus Carneiro, matrícula [redacted] e Plinio Andrade Passos, matricula [redacted] para exercerem as atribuições de fiscal e suplente, respectivamente, do contrato nº 001/2021-SGA, relativo à prestação de serviços gateway de e-mail em nuvem com módulo de inspeção de E-mails entre caixas de correio e serviços online de proteção / filtragem de e-mail para 4.000 caixas postais.

Superintendência de Gestão Administrativa do Ministério Público do Estado da Bahia, 08 de janeiro de 2021.

Frederico Welington Silveira Soares
Superintendente de Gestão Administrativa

sei! assinatura eletrônica

Documento assinado eletronicamente por **Frederico Welington Silveira Soares** em 08/01/2021, às 17:51, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.sistemas.mpba.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0067961** e o código CRC **E1C558E0**.

SUPERINTENDÊNCIA DE GESTÃO ADMINISTRATIVA

DIRETORIA DE GESTÃO DE PESSOAS

LICENÇA PATERNIDADE DEFERIDA					
MAT.	**NOME DO SERVIDOR**	**LEI/ATO**	**QT. DIAS DEFERIDOS**	**INÍCIO**	**TÉRMINO**
[redacted]	CLEBER ADRIANO RODRIGUES FOLGADO	Lei n° 6.677/1994 – Art. 155 Ato Normativo n° 012/2016	20	22/12/2020	10/01/2021

SUPERINTENDÊNCIA DE GESTÃO ADMINISTRATIVA DO MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA, 11 de janeiro de 2021.

RETIFICAÇÃO:
Averbação de tempo de serviço público estadual, publicada no DPJ de 07/03/2006, em favor do ex-servidor, por força do expediente n° 003.0.32198/2019, Parecer n° 202/2020, onde se lê:

Nome	Matrícula	Cargo	Processo	Tempo averbado		Efeitos
GERSONE BATISTA LIMA	[redacted]	Assistente Técnico-Administrativo	003.2.102808/2005	**02 anos, 08 meses e 01 dia** (CTC do INSS de 11/11/2005)	serviço público estadual prestado à Secretaria da Educação - SEC	aposentadoria e adicional de tempo de serviço

Leia-se:

Nome	Matrícula	Cargo	Processo	Tempo averbado		Efeitos
GERSONE BATISTA LIMA	[redacted]	Assistente Técnico-Administrativo	003.2.102808/2005	**02 anos e 07 meses** (considerando o abatimento do período concomitante prestado à SEC e ao MP/BA, qual seja, 01/03/2005 a 01/04/2005, no total de 31 dias.)	serviço público estadual prestado à Secretaria da Educação - SEC	aposentadoria e adicional de tempo de serviço

PROCESSO DEFERIDO PELA SUPERINTENDÊNCIA DE GESTÃO ADMINISTRATIVA:

DESAVERBAÇÃO DO TEMPO DE CONTRIBUIÇÃO AO REGIME GERAL DE PREVIDÊNCIA SOCIAL

Nome	Matrícula	Cargo	Processo/Publicação da averbação	Motivação da desaverbação	Processo/Parecer autorizador da desaverbação	Decisão	Efeito
GERSONE BATISTA LIMA	[redacted]	Assistente Técnico-Administrativo	Processo n° 003.2.102808/2005, DPJ de 07/03/2006.	Requerimento do ex-servidor	003.0.32198/2019. Parecer n° 202/2020, de 26/05/2020	Desaverbação do tempo de contribuição ao regime geral de previdência social relativo ao serviço público estadual e iniciativa privada, constante da CTC do INSS, emitida em 11/11/2005. Tempo de Contribuição: 2.845 dias - 07 anos, 09 meses e 20 dias. Desentranhamento da certidão original do INSS e posterior devolução ao ex-servidor.	Não produziu o efeito de aposentadoria

SUPERINTENDÊNCIA DE GESTÃO ADMINISTRATIVA DO MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA, 11 de janeiro de 2021.

DIRETORIA DE CONTRATOS, CONVÊNIOS E LICITAÇÕES

RESUMO DE CONTRATO DE PRESTAÇÃO DE SERVIÇOS Nº 001/2021 - SGA. Processo SEI: 19.09.02684.0007250/ 2020-58 – Pregão Eletrônico nº 048/2020. Parecer jurídico nº 749/2020. Partes: Ministério Público do Estado da Bahia e empresa HSC Desenvolvimento e Serviços em Tecnologia da Informação LTDA, CNPJ nº 13.103.980/0001-08. Objeto: Prestação de serviços de gateway de e-mail em nuvem com módulo de inspeção de E-mails entre caixas de correio e serviços online de proteção / filtragem de e-mail para 4.000 caixas postais, com o objetivo de proteção anti-spam, anti-malware, anti-phishing, anti-spear phishing (phishing direcionado), tratamento de ameaças avançadas, incluindo sistema de segurança contra ataques dirigidos, com sandbox para verificar arquivos anexos, assim como suporte técnico, implantação e treinamento. Regime de execução: Empreitada por preço global. Valor total: R$ 469.000,00 (quatrocentos e sessenta e nove mil reais). Dotação orçamentária: Unidade Orçamentária/Gestora 40.601/0003 – Ação (P/A/OE) 2002 – Região 9900 - Destinação de Recursos 100 - Natureza de Despesa 33.90.40. Forma de Pagamento: ordem bancária para crédito em conta corrente e agência indicadas pela empresa contratada. Prazo de vigência: 25 (vinte e cinco) meses, a contar da data da sua publicação no Diário da Justiça Eletrônico.

PORTARIA Nº 002/2021

SUPERINTENDENTE DE GESTÃO ADMINISTRATIVA DO MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA, no uso de suas atribuições, RESOLVE designar os servidores laçanã Lima de Jesus Carneiro, matrícula [redacted] e Plinio Andrade Passos, matricula [redacted] para exercerem as atribuições de fiscal e suplente, respectivamente, do contrato nº 001/2021-SGA, relativo à prestação de serviços gateway de e-mail em nuvem com módulo de inspeção de E-mails entre caixas de correio e serviços online de proteção / filtragem de e-mail para 4.000 caixas postais.

Superintendência de Gestão Administrativa do Ministério Público do Estado da Bahia, 08 de janeiro de 2021.

Frederico Welington Silveira Soares
Superintendente de Gestão Administrativa

PROCURADORIAS E PROMOTORIAS DE JUSTIÇA

INQUÉRITO(S) CIVIL(S) / PROCEDIMENTO(S):

PRORROGAÇÃO DO PRAZO DE CONCLUSÃO DE PROCEDIMENTO ADMINISTRATIVO

A Promotoria de Justiça da Comarca de Condeúba/BA, através de seu Promotor de Justiça em substituição, MARCOS ALMEIDA COELHO, no uso de suas atribuições legais, diante da necessidade de prosseguir com as apurações, em virtude da realização de diligências e pendências de respostas a ofícios expedidos, determina a PRORROGAÇÃO, por mais um ano, do prazo de conclusão do Procedimento Administrativo: 003.9.143913/2007

Condeúba, 30 de novembro de 2020.

MARCOS ALMEIDA COELHO
Promotor de Justiça em substituição

PROMOTORIA DE JUSTIÇA DA COMARCA DE CONDEÚBA – BA

Edital 01/2021

O MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA, pelo Promotor de Justiça em substituição na Comarca de Condeúba/BA, no uso de suas atribuições legais, considerando o disposto no Art. 26, § 2º, da Resolução 06/2009, do Colégio de Procuradores de Justiça do Estado da Bahia c/c Art. 10 da Resolução nº 23/2007 do CNMP – Conselho Nacional do Ministério Público, NOTIFICA Cleberson Antonio Ferreira Modena e aos demais interessados, inclusive para efeito de eventual apresentação de razões escritas ou juntada de documentos no prazo de 10 (dez) dias, de que foi Arquivado o Procedimento Preparatório nº 089.9.193218/2017 que visava apurar supostas irregularidades concernentes à representação do Município de Condeúba em processos relativos aos precatórios do FUNDEF, além de ilações sobre possíveis irregularidades nos processos licitatórios por inexigibilidade de licitação correspondentes à sua contratação.

De Vitória da Conquista para Condeúba, 08 de janeiro de 2021.

MARCOS ALMEIDA COELHO
Promotor de Justiça em substituição

3ª Promotoria de Justiça de Dias d'Ávila
Prorrogação de Prazo de Procedimento Administrativo
IDEA nº 111.9.222591/2019
Data da Decisão: 08/01/2021
Área: Infância e Juventude

Trata-se de Procedimento Administrativo instaurado a fim de apurar suposta situação de risco dos menores P.K.S.C. e J.G.S.M.M.. Constato que o prazo inicial de tramitação do Procedimento Administrativo encontra-se vencido desde 02.12.2020, em que pese em vigor Resolução do CNMP que determina a suspensão dos prazos de tramitação dos procedimentos extrajudiciais durante o período da pandemia do COVID-19. Por motivo de ainda existirem diligências a serem realizadas, determino, com fulcro no artigo 11º da Resolução do CNMP nº 174/2017, a prorrogação do presente procedimento administrativo por mais 01 (um) ano, a contar de 02 de dezembro de 2020.

LARA FERRARI FONSECA
Promotora de Justiça