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 HSC DESENVOLVIMENTO E SERVIÇOS EM TECNOLOGIA DA INFORMAÇÃO LTDA, NA FORMA ABAIXO:

CONTRATO Nº 002/2025 - SGA

O MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA, CNPJ n º 04.142.491/0001-66, com sede situada à 5ª Avenida, 750, Centro Administrativo da Bahia - CAB, Salvador - BA, neste ato representado, mediante Ato de Delegação nº 70/2014, pelo Superintendente de Gestão Administrativa **André Luis Sant´Ana Ribeiro**, doravante denominado **CONTRATANTE**, e a **HSC DESENVOLVIMENTO E SERVIÇOS EM TECNOLOGIA DA INFORMAÇÃO LTDA** , CNPJ nº. 13.103.980/0001-08, estabelecida à Rua General João Manoel, num.50, conj. 502, bairro Centro, CEP 90.101-030, representada por **Romulo Giordani Boschetti**, inscrito(a) no CPF/MF nº 82******20, doravante denominada **CONTRATADA**, com supedâneo no quanto disposto na Lei Federal nº 14.133/2021 e na Lei Estadual/Ba nº 14.634/2023, e, ainda, observado o constante no Processo de Licitação, nº 90013/2024, protocolado sob o nº 19.09.00854.0029128/2024-70, o qual integra este instrumento independentemente de transcrição, **CELEBRAM** o presente Contrato, mediante as cláusulas e condições seguintes:

CLÁUSULA PRIMEIRA - DO OBJETO

1.1 O presente instrumento tem por objeto contratação de serviço 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 email 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, pelo período de 36 meses, conforme condições estabelecidas neste instrumento e em seu apenso único.

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

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

CLÁUSULA SEGUNDA – DA VINCULAÇÃO AO EDITAL DO CERTAME LICITATÓRIO

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

CLÁUSULA TERCEIRA – DA DURAÇÃO DO CONTRATO

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

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

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

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

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

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

4.2.1 As comprovações da convocação e da entrega/retirada da nota de empenho poderão ocorrer por quaisquer dos seguintes meios: por meio eletrônico (através de confirmação de recebimento de e-mail), aposição de assinatura (para retirada presencial) ou por Aviso de Recebimento dos correios (quando a entrega for via postal).

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

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

4.4 Para a realização dos serviços é necessário o prévio agendamento junto à Diretoria de Tecnologia da Informação – Coordenação de Assessoramento em Segurança da Informação, através dos contatos telefônicos (71)-3103-0214 e e-mail iassa@mpba.mp.br. A referida unidade será responsável por acompanhar a execução dos serviços;

4.5 O prazo de início da execução do objeto contratual é de até 15 (quinze) dias corridos, contados do dia útil subsequente ao recebimento da Nota de Empenho, contrato ou documento equivalente;

4.6 Os serviços serão prestados observando-se as seguintes condições:

SERVIÇO/ETAPAS	CONDIÇÕES	CRONOGRAMA DE EXECUÇÃO
01	Entrega do licenciamento	5 dias
02	Kick off - Implantação	5 dias
03	Treinamento	5 dias

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

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

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

4.10 A **CONTRATADA** prestará os serviços objeto da contratação com garantia contratual técnica, complementar à garantia gela, observando-se o seguinte:

4.10.1 A contratação de garantia contratual técnica complementar do serviço ou bem empregado em sua execução se justifica por ser uma contratação de uma solução crítica, visando assim o suporte ao serviço de antispam que é essencial para garantir a continuidade deste serviço, mantendo por mais tempo possível o uptime de proteção contra ameaças emergentes, através de suporte técnico especializado e conformidade regulatória. Isso assegura que o MPBA estará devidamente protegido contra os riscos associados ao correio eletrônico, enquanto otimiza seus recursos e minimiza interrupções operacionais.

4.10.2 A garantia contratual complementar deverá ser prestada pelo fabricante e/ou fornecedor;

4.10.3 O prazo de garantia contratual técnica dos serviços, complementar à garantia legal, é de, no mínimo, 36 (trinta e seis) meses, contados a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto;

4.10.4 A garantia perdurará continuamente durante toda a vigência contratual;

4.10.5 As garantias legal e contratual não se sobrepõem, devendo seus prazos serem comados;

4.10.6 A garantia será prestada com o propósito de manter os serviços em perfeitas condições de execução, sem qualquer ônus ou custo adicional ao **CONTRATANTE**;

4.10.7 Uma vez notificado, o Fornecedor deverá responder ao chamado de abertura do **CONTRATANTE** no prazo de 24 (vinte e quatro) horas realizar a reparação ou refazimento dos serviços que apresentem defeitos no prazo de até o próximo dia corrido, contados da abertura do chamado;

4.10.8 O prazo indicado no subitem anterior, durante seu transcurso, poderá ser prorrogado uma única vez, por até o próximo dia corrido, mediante solicitação escrita e justificada do Fornecedor, aceita pelo **CONTRATANTE**;

4.10.9 A garantia legal ou contratual do objeto tem prazo de vigência próprio e desvinculado do prazo de vigência do contrato, permitindo eventual aplicação de penalidades em caso de descumprimento de alguma de suas condições, mesmo depois de expirada a vigência contratual.

CLÁUSULA QUINTA – DO RECEBIMENTO DO OBJETO

5.1 O recebimento provisório dos serviços será realizado mediante termo detalhado emitido pelo fiscal técnico, relativamente ao cumprimento dos prazos de execução e demais exigências de caráter técnico, devendo ocorrer em até **5 dias corridos;**

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

5.2 Os serviços poderão ser rejeitados, no todo ou em parte, inclusive antes do recebimento provisório, quando em desacordo com as especificações constantes neste instrumento e na Proposta de preços, devendo ser refeitos no prazo de **5 dias (cinco)** dias **corridos**, a contar da intimação do fornecedor, às suas custas, sem prejuízo da aplicação das penalidades, cabendo à fiscalização não atestar o recebimento até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório;

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

5.4 Os serviços serão recebidos definitivamente, em até 10 (dez) dias corridos, contados do recebimento provisório, pelo gestor do contrato ou comissão designada pelo Superintendente de Gestão Administrativa, mediante termo detalhado que comprove o atendimento de todas as exigências contratuais;

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

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

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

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

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

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

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

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

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

5.11 O aceite ou aprovação do objeto pelo **CONTRATANTE** não exclui a responsabilidade do fornecedor pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do Contrato.

CLÁUSULA SEXTA – DO PREÇO

6.1 O preço unitário será de R$ 327,00 (trezentos e vinte e sete reais), equivalente à unidade de caixa postal;

6.2 Dá-se ao presente Contrato o valor global de R$ 1.308.000,00 um milhão, trezentos e oito mil reais), equivalente a 4000 unidades de caixa postal, pelo período total de vigência da contratação;
6.3 Nos preços computados neste Contrato estão inclusos todos e quaisquer custos necessários ao fiel cumprimento deste instrumento, inclusive todos aqueles relativos a remunerações, encargos sociais, previdenciários e trabalhistas de todo o pessoal da **CONTRATADA** envolvido na execução do objeto, materiais empregados, inclusive ferramentas e fardamentos, combustíveis, lubrificantes, manutenção, lavagens, estacionamento, depreciação, aluguéis, seguros, franquias, administração, tributos e emolumentos.

CLÁUSULA SÉTIMA - DO PAGAMENTO E DA ATUALIZAÇÃO MONETÁRIA

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

7.2 O faturamento referente ao objeto deste contrato será efetuado em parcela única, após o recebimento definitivo do objeto contratado.

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

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

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

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

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

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

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

7.8 A atualização monetária dos pagamentos devidos pelo **CONTRATANTE**, em caso de mora, será calculada considerando a data do vencimento da obrigação e do seu efetivo pagamento, de acordo com a variação do INPC do IBGE *pro rata tempore,* observado, sempre, o disposto nos **itens 7.4 e 7.4.1.**

7.8.1 Para efeito de caracterização de mora imputável ao **CONTRATANTE**, não serão considerados eventuais atrasos de pagamento no período de fechamento do exercício financeiro do Estado da Bahia, compreendido entre o final do mês de dezembro e o mês de janeiro do exercício subsequente, decorrentes de circunstâncias alheias à vontade das partes, isto é, por força de bloqueio de rotinas no sistema estadual obrigatoriamente utilizado para a execução dos pagamentos devidos pelo **CONTRATANTE**.

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

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

8.1 A concessão de reajustamento ocorrerá após o transcurso do prazo de 01 (um) ano da data do orçamento estimado pela Administração, qual seja, 13 de setembro de 2024, mediante aplicação do IPCA relativo ao período decorrido entre a referida data e a data da efetiva concessão do reajuste;

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

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

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

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

8.2.1. O requerimento de restabelecimento do equilíbrio econômico-financeiro inicial do contrato, nas hipóteses do art. 124, II, "d", ou do art. 135 da Lei Federal nº 14.133, de 2021, deverá ser formulado pelo interessado no prazo máximo de um ano do fato que o ensejou, sob pena de decadência, em consonância com o art. 211 da Lei Federal nº 10.406, de 10 de janeiro de 2002;

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

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

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

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

CLÁUSULA NONA - DA DOTAÇÃO ORÇAMENTÁRIA

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

Código Unidade Orçamentária/Gestora	Ação (P/A/OE)	Região	Destinação de Recursos (Fonte)	Natureza da Despesa
40.101/0021	2002	9900	100	33.90.40

CLÁUSULA DÉCIMA - DO MODELO DE GESTÃO E FISCALIZAÇÃO CONTRATUAL

10.1 Na forma das disposições estabelecidas na Lei Federal nº 14.133/2021 e na Lei Estadual/BA nº 14.634/2023, o **CONTRATANTE** designará servidor(es), por meio de Portaria específica para tal fim, para a gestão e fiscalização deste contrato, tendo poderes, entre outros, para notificar a **CONTRATADA** sobre as irregularidades ou falhas que porventura venham a ser encontradas na execução deste instrumento.

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

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

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

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

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

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

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

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

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

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

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

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

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

10.5.1 Autorizar o início da execução do objeto contratual, deliberando sobre o momento do envio de documentos de formalização tais como documentos ou nota de empenho ordinária ao contratado.

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

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

10.5.4 Deliberar sobre prorrogações de prazos de entre ou execução;

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

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

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

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

CLÁUSULA DÉCIMA PRIMEIRA – DAS OBRIGAÇÕES DA CONTRATADA

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

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

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

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

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

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

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

11.7 Promover a destinação final ambientalmente adequada do dos materiais eventualmente empregados na prestação dos serviços, sempre que a legislação assim o exigir;

11.8 Prestar ao **CONTRATANTE**, sempre que necessário, esclarecimentos, fornecendo toda e qualquer orientação necessária;

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

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

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

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

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

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

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

11.15.1 Comunicar ao **CONTRATANTE**, no prazo de 24 (vinte e quatro) horas, qualquer ocorrência anormal relativa à execução;
11.16 Prestar todo esclarecimento ou informação solicitada pelo **CONTRATANTE** ou por seus prepostos, garantindo-lhes o acesso, a qualquer tempo, aos documentos relativos à execução do objeto;

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

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

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

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

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

CLÁUSULA DÉCIMA SEGUNDA – DAS OBRIGAÇÕES DO CONTRATANTE

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

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

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

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

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

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

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

12.8 Notificar previamente ao fornecedor, quando da aplicação de penalidades;
12.9 Atestar as notas fiscais/faturas emitidas pelo fornecedor, recusando-as quando inexatas ou incorretas, efetuando todos os pagamentos nas condições pactuadas;

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

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

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

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

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

13.709/2018

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

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

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

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

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

CLÁUSULA DÉCIMA QUARTA - DA GARANTIA DA EXECUÇÃO

Não será exigida garantia da execução contratual.

CLÁUSULA DÉCIMA QUINTA – DAS INFRAÇÕES E DAS SANÇÕES ADMINISTRATIVAS

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

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

15.2.1 Der causa à inexecução parcial do contrato;

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

15.2.3 Der causa à inexecução total do contrato;

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

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

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

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

15.2.8 Praticar ato fraudulento na execução do contrato;

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

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

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

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

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

15.3.3 **Declaração de inidoneidade para licitar e contratar**, quando praticadas as condutas descritas nos itens 15.2.5 a 15.2.10, acima, bem como nas alíneas 15.2.2 a 15.2.4, que justifiquem a imposição de penalidade mais grave (art. 156, §5º, da Lei Federal nº 14.133/21);

15.3.4 Multa:

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

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

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

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

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

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

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

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

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

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

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

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

15.7. Na aplicação das sanções serão considerados:

15.7.1 A natureza e a gravidade da infração cometida;

15.7.2 As peculiaridades do caso concreto;

15.7.3 As circunstâncias agravantes ou atenuantes;

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

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

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

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

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

Empresas Punidas (Cnep), instituídos no âmbito do Poder Executivo Federal;

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

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

CLÁUSULA DÉCIMA SEXTA – DAS ALTERAÇÕES CONTRATUAIS

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

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

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

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

CLÁUSULA DÉCIMA SÉTIMA – DA EXTINÇÃO DO CONTRATO

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

17.1.1. O contrato pode ser extinto antes do prazo nele fixado, sem ônus para o **CONTRATANTE**, quando este não dispuser de créditos orçamentários para sua continuidade ou quando entender que o contrato não mais lhe oferece vantagem;

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

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

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

17.2.1 A extinção do contrato poderá ser:

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

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

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

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

17.3.1 Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

17.3.2 Relação dos pagamentos já efetuados e ainda devidos;

17.3.3 Indenizações e multas.

17.4 O contrato poderá ser extinto, ainda:

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

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

CLÁUSULA DÉCIMA OITAVA – DA AUSÊNCIA DE VÍNCULO EMPREGATÍCIO

18.1 A utilização de mão de obra, pela **CONTRATADA**, para execução dos serviços objeto do presente contrato não ensejará, em nenhuma hipótese, vínculo

empregatício com o **CONTRATANTE**; **CLÁUSULA DÉCIMA NONA – DA PUBLICIDADE**

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

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, não transfere ao **CONTRATANTE** a responsabilidade pelo seu pagamento, nem poderá onerar o objeto do contrato;

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

21.4 Fica assegurado ao **CONTRATANTE** o direito de alterar unilateralmente o Contrato, mediante justificativa expressa, nas hipóteses previstas na Lei Federal 14.133/21 e na forma de Lei Estadual de nº 14.634/23 para melhor adequação às finalidades de interesse público, desde que mantido o equilíbrio econômico-financeiro original do contrato e respeitados os demais direitos da **CONTRATADA**;

21.5 Não caracterizam novação eventuais variações do valor contratual resultantes de reajustamento/revisão de preços, de compensações financeiras decorrentes das condições de pagamento nele previstas ou, ainda, de alterações de valor em razão da aplicação de penalidades;

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

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

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

Salvador, 2025.

APENSO ÚNICO

ESPECIFICAÇÕES TÉCNICAS DETALHADAS Especificação Técnica de Solução de Segurança Anti-Spam e E-mail

Gateway

Objeto:

Contratação de solução de Filtragem de conteúdo de E-mail (anti-spam), para 4.000 caixas postais, incluindo sistema de segurança contra-ataques dirigidos, bem como suporte técnico, implantação e treinamento, pelo período de 36 meses.

Especificação Técnica

Nuvem Dedicada

Deve ser apresentada para o órgão servidores dedicados para gestão, permitindo que o administrador possa gerenciar todas as funcionalidades do sistema, sem restrições, nem limitações, de qualquer lugar através da Internet;

Características da Nuvem Dedicada

1. Por questão de desempenho, garantia de sigilosidade das informações e atendimento ao LGPD (Lei Geral de Proteção de Dados), através da instrução normativa nº5 de 30 de agosto de 2021 da legislação brasileira, o(s) datacenter(s) deve(m) estar localizado(s) no Brasil:

> *Art. 18. Os dados, metadados, informações e conhecimentos produzidos ou custodiados pelo órgão ou pela entidade, transferidos para o provedor de serviço de nuvem, devem estar hospedados em território brasileiro, observando-se as seguintes disposições:*
>
> *I - pelo menos uma cópia atualizada de segurança deve ser mantida em território brasileiro; II - a informação sem restrição de acesso poderá possuir cópias atualizadas de segurança fora do território brasileiro, conforme legislação aplicável; III - a informação com restrição de acesso prevista na legislação e o documento preparatório não previsto no inciso II do caput art. 17, bem como suas cópias atualizadas de segurança, não poderão ser tratados fora do território brasileiro, conforme legislação aplicável; e IV - no caso de dados pessoais, deverão ser observadas as orientações previstas na Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de*

Dados Pessoais - LGPD, e demais legislações sobre o assunto.

2. O serviço oferecido em nuvem deve prover no mínimo dois servidores dedicados para a parte de filtragem dos emails, com IP's distintos;
3. Os servidores utilizados na infraestrutura da solução em nuvem devem possuir alta disponibilidade, isto é, se cair um servidor de filtragem o(s) outro(s) devem assumir toda a carga e garantir a entrega sem sobrecarga do sistema;
4. Os servidores utilizados na filtragem dos emails, devem efetuar LoadBalance (balanceamento automático de carga), de forma transparente e sem intervenção do administrador;
5. Deve permitir configuração de múltiplas entradas de MX, uma entrada para cada IP a fim de garantir maior disponibilidade;
6. Deve ter garantia de uptime (garantia de funcionamento do datacenter) de no mínimo 99,7%;
7. Deve manter os registros (logs) por pelo menos 6 meses, atendendo o Marco Civil da Internet no Brasil, sendo acessível ao administrador na própria console de

gerenciamento (no modo gráfico, sem uso de linha de comando), sem necessidade de solicitar ao fabricante a liberação desses logs;

Da Plataforma

1. A solução Antispam deve possuir controle de caixas postais e fluxo de análise de mensagens/dia ilimitadas, de acordo com os recursos de hardware disponíveis;
2. Para maior facilidade de instalação e configuração, a solução deve conter um Wizard de instalação em modo gráfico, orientando o processo passo a passo em língua portuguesa do
   Brasil;
3. 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;
4. A licença de uso deve atingir um número de **4000** caixas postais;
5. Toda as funcionalidades e configurações do produto devem ser efetuadas via Interface Gráfica, sem necessidade de uso de linha de comando (CLI) ou outro recurso que não seja nativo da Interface Gráfica do Produto, através de browsers;
6. O sistema operacional deve ser para uso próprio em sistema de proteção a email, não sendo aceito sistema onde simplesmente é instalado um programa de filtragem de email rodando sobre sistema operacional "genérico" ou de distribuição livre, tais como BSD e correlatos;
7. Deve ser capaz de filtrar o tráfego de correio, bloqueando a entrada de vírus, spyware, worms, trojans, SPAM, phishing, e-mail marketing, e-mail adulto ou qualquer outra forma de ameaça virtual;
8. Deve permitir alta disponibilidade das funções de filtragem, de maneira assegurar que o serviço de correio nunca pare por falha da solução;
9. A solução deve suportar o processamento de no mínimo 20.000 (vinte mil) conexões simultâneas e 160.000 (cento e sessenta mil) mensagens por hora;
10. A licença de uso do software deve possuir **36 meses** de atualização do fabricante compreendendo os seguintes módulos:
    a. 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;
    b. Direito de uso da versão mais atual do produto licenciado caso esta esteja disponível pelo fabricante, bem como atualizações de recursos e melhorias dentro da mesma versão;
    c. Acesso a base de inteligência global do fabricante para análise online de ameaças;
    d. Suporte técnico para todos os módulos da solução
11. Analisar mensagens, no mínimo, por meio dos seguintes métodos:
    11.1 Proteção dinâmica por reputação;
    11.2 Assinaturas de spam;
    11.3 Filtros de Vírus;
    a) A verificação de vírus, além da técnica tradicional (por assinatura), também deve ser feito através de BigData do fabricante, bem como utilização de método Fuzzy Hash ou Similar para detecção de similaridades e detecção de possível variante de malware;
    b) Possuir no mínimo de duas engines distintas de antivírus, sendo um do próprio fabricante e a outra engine de outro fabricante, ambos já devidamente licenciados para uso simultâneo;
    11.4 Filtros de anexos;
    11.5 Filtros de phishing;
    11.6 Análise heurística;
    11.7 Análise do cabeçalho, corpo e anexo das mensagens;
    11.8 E-mail bounce;
    11.9 Dicionários pré-definidos e customizados com palavras e expressões regulares;
    11.9.1 Já deve vir acompanhando de dicionários pré-estabelecidos, para possível utilização (não sendo aceito a inserção dos dicionários posteriormente):
    i) Número de cartão de crédito; ii) Número de passaporte brasileiro;
    iii) CNPJ;
    iv) Placa de Carro padrão Mercosul;
    v) CNH (Carteira Nacional de Habilitação); vi) RG e CPF;
12. Deve permitir ao administrador escolher a forma de uso de certificado SSL, entre eles: a. Auto-assinado;
    b. Importação do certificado SSL da empresa;
13. Deve possuir mecanismo de backup e recuperação da configuração da solução na própria interface gráfica do produto, sem necessidade de linha de comando;
14. Deve possuir capacidade de envio de backup via FTP e SFTP, sendo configurado diretamente na interface gráfica da solução (sem necessidade de qualquer configuração em linha de comando);
15. Deve possibilitar manter na própria ferramenta o backup da configuração da solução por período mínimo de 365 dias, possibilitando recuperação do mesmo a qualquer momento;
16. Os manuais necessários à instalação e administração da solução, devem ser originais do fabricante e constar no mínimo os seguintes idiomas: Português do Brasil ou Inglês;
17. A interface de administração do sistema deve ter suporte a no mínimo um dos seguintes idiomas:
    a. Português do Brasil;
    b. Inglês.
18. A interface de **quarentena do usuário** deve suportar o idioma Português do Brasil;
19. Deve possuir banco de dados relacional para armazenamento dos registros de acesso, logs de sistema e configurações. Caso a solução necessite de banco de dados específico e proprietário, as licenças deste deverão ser fornecidas pela contratada junto com a solução ofertada sem ônus para o contratante. Não serão aceitas soluções baseadas em armazenamento de Logs em formato Texto;
20. Deve possuir capacidade de configuração de roteamento de mensagens para múltiplos domínios de destino;
21. Deve permitir a configuração de múltiplos domínios, com aplicação de regras de forma independente para cada um dos domínios;
22. Ter a capacidade de processar o tráfego de entrada e de saída de mensagens no mesmo equipamento, com base no IP e domínio de origem da mensagem, permitindo criar filtros e ações diferenciadas para cada sentido;
23. A solução deve ser capaz de efetuar a saída de e-mails indicando um IP específico para a saída de mensagens, isto é, possuir a capacidade de redirecionar as mensagens de saída por IP's diferentes para cada domínio cadastrado no sistema se o administrador assim desejar;
24. A solução deve permitir, no mínimo, criação de regras por:
    a. Grupos de usuários;
    b. Domínios;
    c. Range de IP;
    d. IP/Rede;
    e. Remetentes específicos;
    f. Destinatários específicos;
    g. Grupos de LDAP.

25. Tratar e analisar mensagens originadas e recebidas possibilitando a aplicação de regras e políticas customizáveis, além de diferenciadas por sentido de tráfego;
26. 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” e “ou”;
27. A console de gerenciamento deve ser acessada através de protocolo seguro (HTTPS – HyperText Transfer Protocol Secure) com no mínimo as seguintes funcionalidades:
    a. Administração centralizada de todas as regras e filtros integrantes da solução;
    b. Data e hora do último update de assinaturas do antivírus em uso, bem como a data e hora da última tentativa de update;
    c. Controle de acesso de usuários, com diferentes privilégios de configuração;
    d. Criação de relatórios, gráficos e estatísticas, com suporte a múltiplos domínios;
    e. Gerência das áreas de quarentena pelo administrador e possibilidade do usuário gerenciar sua área de quarentena.
28. Deve possuir administração via shell, através de SSH para CLI (command line interface), para execução de comandos de administração e suporte;
29. Deve ser capaz de utilizar os protocolos de transferência de arquivos SCP e FTP;
30. Suporte à assinatura e validação de autenticidade de mensagens através de Domains Keys, DKIM e SPF;
31. Permitir efetuar controle profundo dos anexos das mensagens, podendo tomar ações diferenciadas para:
    a. Conteúdo do anexo;
    b. Mime-Type do anexo;
    c. Extensão do anexo;
    d. Nome completo do anexo;
    e. Nome parcial do anexo;
    f. Expressão regular;
    g. Tamanho do anexo;
    h. Anexos compactados com senha;
    i. Quantidade de níveis de compactação no mesmo anexo.
32. Deve possuir um sistema de Disaster e Recover ao qual é efetuado o upload de um arquivo de backup e restauração do mesmo automaticamente;
33. Prover funcionalidade de armazenagem e retorno de, no mínimo, as 5 (cinco) últimas mudanças de configuração, sem necessidade de restauração de back-up, nem parada quanto ao funcionamento da solução;
34. Possuir a função de abertura de relay automático para empresas que usam Microsoft Office 365, sem necessidade de cadastro de IP´s ou DNS da Microsoft para abertura de relay.
35. Deve possuir sistema de diagnóstico via interface WEB, com no mínimo a execução dos seguintes testes:
    a. Teste de Conectividade TCP – Informando o Host e a Porta a serem testados;
    b. Teste de Conectividade ICMP – Informando o Host a ser testado;
    c. Teste de DNS – Informando o Host ou o Domínio a serem testados;
    d. Teste de Envio de E-mail;
    e. Teste de Conectividade com o fabricante (para isso, testa-se as portas e endereços necessários de comunicação junto ao fabricante, apresentando o resultado dessa comunicação ao administrador da solução);
    f. Teste de TRACEROUTE;
    g. Teste de DNS Reverso;
    h. Teste de SPF, para checar se tem registro para um determinado domínio;
    i. Teste de DKIM, para checar se tem registro para um domínio;
    j. Teste de DMARC, para checar se tem registro para um domínio;
    k. Teste de portas de Saída utilizadas pelo sistema;
    l. Teste de conectividade com serviços Microsoft, para plataforma Microsoft Office 365.
36. Deve ter a capacidade de controle sobre os serviços executados no sistema, com a ação de: parar, inicializar ou reinicializar. O controle dos serviços devem ser sobre no mínimo os seguintes itens:
    a. Serviço de antivírus;
    b. Serviço de MTA;
    c. Serviço de Banco de Dados;
    d. Serviço de SMNP.
37. Deve permitir a instalação de agentes/plug-ins (tanto no equipamento utilizado no gerenciamento, quanto nos agentes que fazem a filtragem) para monitoramento com sistemas de terceiros, com no mínimo:
    a. Zabbix;
    b. Nagios.
38. Deve ter integração com sistemas de Detecção e Resposta Estendida (XDR);
39. Deve permitir integração com sistemas SIEM (Security Information and Event Management);
40. Para maior segurança e conformidade, deve possuir controle de acesso a solução, restringido a liberação do seu uso, associando o perfil de acesso com IP e/ou rede liberada;
41. Para barrar acessos indevidos, a solução ofertada deve possuir sistema de login com autenticação de dois fatores nativo, sem necessidade de instalação de módulo extra ou utilizar software de terceiros, sendo no mínimo compatível com os seguintes autenticadores:
    a. Google Authenticator;
    b. Microsoft Authenticator;
42. Deve permitir que o administrador crie listas de remetentes confiáveis e remetentes a serem bloqueados a nível de conexão (camada MTA). Esta lista deve ser possível por:
    a. IP de Origem;
    b. Domínio;
    c. Endereço de Email de Origem (do envelope do email);
43. O sistema deve identificar e bloquear ataques que exploram vulnerabilidades na decodificação de domínios que utilizam IDN (Internacionalized Domain Names), incluindo URL encurtadas, sendo compatível com RFC 5891, RFC 5892, RFC 5893 e RFC 5894;
44. Para melhor ajuste de desempenho da ferramenta, a solução deve permitir ao administrador alterar a quantidade de memória utilizada no Cache do Banco de Dados, direto, através da interface gráfica (GUI), sem a necessidade de usar linha de comando;
45. Deve possuir indicação de tempo gasto por cada módulo utilizado na análise do email, no mínimo indicando os tempos de processamento de:
    a. Antivírus;
    b. Cálculo de pontuação de SPAM;
    c. Análise dos anexos;
    d. Tempo total de processamento do email;
46. Possuir no manual ou no sistema de ajuda (help) do produto a indicação das assinaturas utilizadas para cálculo de spam no email, bem como a explicação

de cada uma delas, para que o administrador possa saber o motivo da formação da pontuação no email;

47. Seguindo boas práticas de segurança, a solução deve ser alinhada ao Framework MITRE ATT&CK;
48. Se a solução ofertada for do tipo SaaS (software como serviço), utilizando a estrutura do fabricante, para garantia da idoneidade de uso do Datacenter e auditoria constante, o mesmo deve comprovar possuir certificação ISAE 3402 e ISO 27001;
49. Se a solução ofertada for do tipo SaaS (software como serviço), o sistema deverá manter os registros (logs) por pelo menos 6 meses, atendendo o Marco Civil da Internet no Brasil, sendo acessível ao administrador na própria console de gerenciamento (no modo gráfico, sem uso de linha de comando), sem necessidade de solicitar ao fabricante a liberação desses logs;

Da alta disponibilidade

50. Suportar Cluster de Alta Disponibilidade na forma de Cluster Ativo-Ativo ou Load Balance através do registro MX e/ou sistemas de balanceamento proprietário, assegurando as funções de filtragem que o serviço de recebimento, processamento e entrega das mensagens não pare por falha na solução, sem necessidade de aquisição de pacotes de softwares, equipamentos, instalação de módulos extras ou necessidade de licenças extras. O sistema de cluster deve ser nativo na solução tanto no modo Ativo-Ativo, quanto no modo Ativo-Passivo;
51. Deve permitir a configuração em Cluster com appliances físicos ou virtualizados em DataCenters distintos;
52. Deve permitir a formação de cluster com appliances físicos e appliances virtuais de forma mista.
53. A criação e configuração do Cluster deve ser efetuada através da interface gráfica do gerenciador da solução, sem necessidade de uso de linha de comando e edição do DNS interno, edição manual do arquivo host ou criação de rotas manuais;
54. O sistema deve permitir o gerenciamento de múltiplos clusters da solução em um único ambiente, sem necessidade de abertura de novas telas e/ou instalação de novos softwares ou recursos para tal finalidade;
55. Administração centralizada de múltiplos nós de filtragem em uma única interface web, independente se estiver em modo cluster de alta disponibilidade ou load balance de forma que o gerenciamento e a replicação de políticas do cluster também seja feita de forma centralizada;
56. A administração de todo cluster deve ser feita através de um único IP de destino, não sendo permitido a gestão de regras de forma descentralizada;
57. Possuir capacidade de replicação automática das configurações e balanceamento de carga através um único Virtual IP;
58. O cluster funcionando no modo ativo-ativo, se ocorrer a queda de um dos nodes que compõe o cluster, a solução deve garantir a integridade das informações sem nenhuma perda. Essa funcionalidade deve ser nativa da ferramenta, sem necessidade de aquisição de módulos extras para isso;
59. A inclusão de novos nodes no cluster deve ser efetuado através da interface gráfica de gerenciamento (GUI), sem necessidade de utilização de linhas de comando;
60. Deve permitir o redirecionamento de todo o tráfego de saída de emails para um ponto de filtragem específico, em vez de entregar direto para o gateway padrão. Essa função deve ser possível diretamente pela interface gráfica da ferramenta, sem necessidade de linha de comando, nem criação de rota manual;

Do Gerenciamento

61. O acesso à interface de administração deve possuir diferentes níveis de permissionamento, de forma granular, permitindo que sejam configurados perfis diferentes, por endereços de email e domínio permitidos;
62. O sistema deve possuir ainda, no mínimo, os perfis pré-definidos:
    a. Administrador: Com acesso total às configurações da solução;
    b. Administrador: Com acesso total às configurações da solução sem acesso à leitura dos e-mails armazenados tanto na quarentena como mensagens auditadas;
    c. Auditor: Com acesso a visualização dos e-mails armazenados para auditoria;
    d. Operador: Com acesso à administração da quarentena e gerenciamento da “Blacklist e Whitelist”;
    e. Usuário: Possui a capacidade de administrar sua “Blacklist e Whitelist”, individualmente, bem como sua área de quarentena individual.
63. Permitir a criação de grupos, para posterior aplicação de regras. Os grupos poderão ser criados através das seguintes métricas:
    a. E-mails;
    b. Domínios;
    c. IP’s;
    d. Range de IP;
    e. Expressão Regular;
    f. Usuários;
    g. Listas de distribuição;
    h. Grupos de LDAP.
64. Permitir que o administrador inclua exceções a nível de conexão (MTA), mesmo que somente seja feita a verificação da reputação da origem e/ou RBL a nível de MTA, devendo ser no mínimo exceção por:
    a. IP;
    b. Hostname;
    c. Domínio;
65. Deve permitir ao administrador ativar e desativar a análise de RBL (remote block list/realtime blackhole list) na camada de MTA (nível de conexão) e na camada de processamento (durante análise de cálculo de pontuação de spam), bem como escolher quais listas de RBL serão utilizadas para estas análises;
66. Deve possuir sistema de whitelist e blacklist, ao qual permita ao administrador incluir registros de whitelist e/ou blacklist através de Wizard (sem necessidade de digitar endereços de email, domínios ou IPs), dessa forma reduzindo possíveis erros de entrada de registros;
67. Permitir ao administrador trabalhar com os registros de blacklist e whitelist, no mínimo por: a. Expressão Regular;
    b. Domínio;
    c. Sub-domínio;
    d. IP;
    e. E-mail;
68. Para melhor desempenho de entrega dos e-mails, deve permitir ao administrador criar fila personalizada de e-mails, separado por domínios, sendo possível ao administrador a parametrização de:
    a. Número de processor por fila;
    b. Timeout de conexão por fila;
    c. Tempo de reinício de envio (em segundos);
    d. Número máximo de destinatários por mensagem;

Alertas e logs da solução

69. O sistema deve permitir ao administrador configurar o tempo de retenção dos logs, bem como capacidade para manter por período mínimo de 365 dias;
70. Deve enviar notificações por e-mail ao administrador, caso as atualizações não tenham sido realizadas com sucesso;
71. A solução deve ser capaz de gerar notificações a remetente e/ou destinatário com mensagem de alerta customizável;
72. Possuir registro de log de TODAS as ações executadas na interface de administração para fins de auditoria. Esse log deve ser de fácil acesso para

obtenção do mesmo, não sendo necessário acionamento da fabricante da solução;

73. Possuir mecanismo de alerta por e-mail quando houver nova atualização do sistema e sobre o status do processo de atualizações;
74. Deve possuir capacidade de envio dos logs de um nó específico ou de todo o cluster para um servidor de syslog ou de SIEM. Também deve ser possível selecionar os logs a serem enviados, no mínimo, para as opções abaixo:
    a. Emergency;
    b. Alert;
    c. Critical;
    d. Error;
    e. Warning;
    f. Notice;
    g. Informational;
    h. Debug.
75. Deve ser possível enviar alertas por e-mail e pelo protocolo SNMP caso ocorra consumo excessivo de algum recurso do sistema. Os sistemas monitorados para envio dos alertas devem ser, no mínimo:
    a. Espeço em disco;
    b. Filas de e-mail;
    c. Memória;
    d. Processador;
    e. Serviço de Filtragem;
    f. Atualização do sistema de segurança;
    g. Antivirus e Antispam;
    h. Ponto de acesso indisponível.

Das Funcionalidades para o Usuário Final

76. 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;
77. A interface do usuário final deve estar no idioma configurado pelo administrador, sendo no mínimo os seguintes idiomas:
    a. Português do Brasil.
78. O usuário final deve ser capaz de incluir e remover endereços em sua lista pessoal de bloqueio ou de liberação de e-mails;
79. 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”;
80. O usuário final deve ser capaz de solicitar liberação de uma mensagem ao administrador, caso a mensagem contenha conteúdo considerado malicioso ou bloqueado por outro critério qualquer, o qual não permita que o usuário final a libere;
81. O usuário deverá ser capaz de selecionar qual o idioma utilizado na sua interface administrativa, sendo no mínimo os seguintes idiomas:
    a. Português do Brasil;
    b. Inglês;
    c. Espanhol;

De sistemas de segurança

82. Deve seguir os preceitos indicados pelo Framework MITRE ATT&CK;
83. Prover mecanismo nativo para detecção, prevenção e bloqueio de diversos ataques sobre vulnerabilidade do protocolo SMTP, entre eles no mínimo:
    a. SMTP Smuggling - CVE-2023-51764;
84. Conforme indicado pelo CTIR Gov (Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Governo), deve ser compatível com o padrão TLP (Traffic Light Protocol);
85. A solução deve ser capaz de bloquear ataques de negação de serviço (Denial of Service);
86. 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/SSL, permitindo configurar domínios onde o TLS é mandatório;
87. A solução deverá possuir a capacidade de executar as seguintes ações:
    a. Limitar o número de conexões TCP permitidas através de um valor configurável;
    b. Rejeitar a conexão SMTP que se caracterize como "flooding".
88. Deve ser capaz de efetuar a filtragem do tráfego de correio eletrônico bloqueando a entrada e saída de:
    a. Vírus;
    b. Spyware;
    c. Worms;
    d. Trojans;
    e. Spam;
    f. Phishing;
    g. E-mail Marketing, ou qualquer outra forma de ameaça virtual.
89. Deve possuir controle total da comunicação permitindo restringir:
    a. IP reverso mal configurado;
    b. Domínios inexistentes;
    c. Permitir identificar e bloquear e-mails vindos de domínios recentemente cadastrados.
90. Deve permitir ao administrador criar filtros e assinaturas, bem como realizar atualização automática das mesmas, em frequência de consulta configurada pelo administrador.
91. Permitir criação de políticas customizadas para tratamento de spam, vírus e filtragem de conteúdo, de acordo com o destinatário da mensagem;
92. Permitir configurar ações diferenciadas sobre as mensagens suspeitas, incluindo: a. Aceitar;
    b. Colocar em quarentena;
    c. Inserir tag personalizada no assunto;
    d. Marcar o cabeçalho.
93. A solução deve ser capaz de tomar as seguintes ações sobre as mensagens:
    a. Alterar o assunto da mensagem;
    b. Adicionar cabeçalhos para rastreamento;
    c. Descartar a mensagem;
    d. Colocar em uma determinada área de quarentena definida pelo administrador.
94. Deve permitir a criação de regras baseadas no idioma que as mensagens foram escritas, com capacidade de identificar no mínimo, português, inglês e espanhol;

95. Deve permitir a criação de regras baseadas por país;
96. Possuir a capacidade de criar filtros personalizados usando expressões regulares;
97. Permitir criação de listas negras e listas brancas, com opção por domínio, subdomínio, endereço de e-mail e endereço IP;
98. Deve prover um mecanismo que impeça a sua utilização como retransmissor de mensagens originadas externamente (relay);
99. 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;
100. 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”;
101. 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: a. IP reverso e localização;
    b. Registro em blacklists mundiais;
    c. Histórico do IP registrados em RBL’s;
102. 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;
103. Deve ser capaz de realizar Reverse DNS LookUp (rDNS), para validação de fontes de email;
104. Deve possuir suporte ao bloqueio de conexões de e-mails nocivos durante o diálogo SMTP, permitindo a economia de banda, armazenamento e otimização de processamento da solução, em especial baseado em lista local de bloqueio de conexão por:
    • IP;
    • E-mail;
    • Domínio;
    • RBL’s;
105. Deve permitir que o administrador do sistema cadastre novas RBL’s para serem utilizadas a nível de conexão SMTP;
106. 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 emails na saída – quando tem algum e-mail de saída que não esteja com o domínio do órgão como remetente). Por ser um ataque frequente, essa proteção deve ser nativa da solução, bastando o administrador ativar a regra, sem necessidade de criação de regra customizada para isso;
107. 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;
108. Possuir mecanismo de *“Spam Throttling*” permitindo ao administrador limitar o fluxo de mensagens recebidas de origens com baixa reputação;
109. 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;
110. Possuir funcionalidade de verificação de DMARC (Domain-based Message Authentication Reporting & Conformance);
111. Possuir controle de surtos (Outbreak), penalizando o remetente por um tempo configurável pelo administrador ao detectar:
    a. Número excessivo de spams (configurado pelo administrador) oriundos de uma mesma fonte de e-mail;
    b. Número excessivo de vírus (configurado pelo administrador) oriundos de uma mesma fonte de e-mail;
    c. Número excessivo de ataques de dicionário (configurado pelo administrador) oriundos de uma mesma fonte de e-mail;
112. Deve possuir apresentação de ameaças detectadas em tempo real. Nesse sistema de detecção de ameaças em tempo real, deve ser possível identificar:
    a. Fontes de ataques;
    b. Ameaças encontradas;
113. Deve permitir ao administrador definir a restrição de acesso a interface gráfica da solução, atrelando perfis de usuários a redes/IP’s, dessa forma restringindo o acesso somente a redes e máquinas autorizadas;

Da quarentena

114. 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;
115. Deve possibilitar a gestão de quarentena pelos administrados de forma que o mesmo possa 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;
116. Caso uma mensagem seja bloqueada ou rejeitada, a solução deverá informar também a razão do bloqueio e quais regra foram ativadas;
117. A interface deve permitir identificar quais Regras do Modulo de AntiSpam foram ativadas e qual sua pontuação, a fim de permitir ao administrador a elaboração de regras granulares, sem necessidade do administrador efetuar busca de histórico em logs;
118. A solução deve suportar a criação de áreas de quarentena personalizadas para usuários específicos;
119. Para maior segurança, as áreas de quarentenas devem ser armazenadas de forma criptografadas, permitindo ao administrador selecionar a cifra de criptografia a ser utilizada, com no mínimo as seguintes opções de cifras de criptografia:
    a. Blowfish;
    b. Serpent;
    c. Rijindael;
    d. AES;
    e. Twofish;
120. Deve permitir que o tempo de armazenamento da quarentena seja individual por cada área de quarentena;
121. Deve permitir a visualização do resumo de todas as áreas de quarentena e volume de mensagens;
122. 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;
123. Possibilitar ao administrador selecionar o período de expiração das mensagens na quarentena, por exemplo: manter as mensagens das últimas 72 horas, dessa forma ao ultrapassar esse limite, o sistema automaticamente começará a apagar os e-mails quarentenados mais antigos;
124. O tempo de armazenamento da quarentena deve ser individual por área de quarentena, devendo também permitir armazenamento por tempo “indeterminado”;
125. Possibilitar ao administrador selecionar o rotacionamento das mensagens em quarentena por tamanho da quarentena e por quantidade de emails retidos, por exemplo limitar uma quarentena a 100GB ou limitar a 500 emails retidos, sendo que ao ultrapassar o limite deste tamanho ou quantidade, o sistema automaticamente começará a apagar os emails quarentenados mais antigos;
126. O administrador ao criar uma quarentena customizada, deverá ter a capacidade de selecionar quais usuários poderão ter acesso a ela;
127. Pelo sigilo da informação, permitir que seja selecionada quais quarentenas customizadas somente sejam acessíveis a determinados administradores, permitindo a granularidade de acesso destas quarentenas.

Dos Usuários e Grupos

128. 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”). Não serão aceitos a integração do

LDAP ou Microsoft Active Directory através de agentes instalados em servidores ou máquinas locais no ambiente da contratante;

129. Permitir criação de conectores para múltiplos serviços de diretório, por exemplo conector para servidor LDAP e outro conector para Microsoft Active Directory;
130. Possuir a funcionalidade de filtrar individualmente, baseado em políticas definidas por domínio, subdomínio, grupo de usuários e usuário individual, de forma integrada com ferramentas de LDAP, mesmo que a mensagem seja destinada a múltiplos destinatários, em categorias distintas;
131. 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;
132. Integração nativa com o Microsoft Exchange;
133. Possibilitar a customização de regras e políticas por usuários ou grupos;
134. A solução deverá permitir a configuração do intervalo de sincronismo com o serviço de diretório;
135. Permitir atrelar grupos a regras específicas de rotas, por exemplo: Não aplicar determinada regra do módulo de anti-vírus para os e-mails que vierem de um determinado domínio, sendo que esta regra somente será aplicada a um grupo específico de usuários.

Dos relatórios

136. Deve permitir a geração de relatórios de todos os nodes do cluster de forma centralizada através de uma única interface web no console de gerenciamento;
137. Deve ser capaz de gerar relatórios gráficos e agendar o envio dos mesmos a usuários específicos via e-mail;
138. Deve ser capaz de gerar relatórios por data ou por um intervalo de tempo específico;
139. Deve ser possível configurar um período para a retenção dos dados utilizados para geração dos relatórios;
140. Capacidade de criar relatórios contendo no mínimo as seguintes informações:
    a. Sumário de mensagens;
    a. Relatório de Volume de Mensagens por Data;
    b. Principais origens de spam por domínio, endereço de e-mail;
    c. Principais destinos de spam por domínio, endereço de e-mail;
    d. Principais origens de vírus;
    e. Principais fontes de ataque;
    a. Relatório de Top E-mail Relays;
    b. Relatório de Top Remetentes por Quantidade;
    c. Relatório de Top Remetentes por Volume;
    d. Relatório de Top Destinatário por Quantidade;
    e. Relatório de Top Destinatário por Volume;
    f. Estatísticas da quarentena;
    g. Conexões completadas X bloqueadas;
    h. Relatório de tráfego;
    i. Principais destinatários de Spam;
    j. Principais destinatários de e-mail;
    k. Top Ataques por fraude de e-mail / tentativa de spoof.
141. Permitir filtros de relatórios com definição de origem e destinos específico;
142. Possuir relatórios estatísticos de conexões, ameaças, quarentena e SPAM;
143. Deve apresentar estatísticas e monitoramento em tempo real (online) de e-mails com base em gráficos;
144. Os relatórios, no mínimo, devem poder ser filtrados por:
    a. Período de tempo;
    b. Ponto de Filtragem que o e-mail passou;
    c. De;
    d. Para;
    e. Qual a classificação que a mensagem atingiu, dentre eles no mínimo: a. DLP;
        a. Provável SPAM;
        b. SPAM;
        c. Vírus;
        d. Conteúdo Bloqueado;
        e. Whitelist;
        f. Blacklist;
        g. Tamanho Excedido;
        h. Phishing.
    f. Relatório para um único usuário ou Domínio.

Rastreamento das mensagens

145. Permitir o rastreamento de mensagens, independente de qual equipamento do cluster processou, de forma centralizada e por meio da interface de gerenciamento HTTPS (não será aceito pesquisa via linha de comando);
146. O rastreamento deve ser possível através de qualquer um dos seguintes campos: a. ID da mensagem;
    b. E-mail do Remente;
    c. E-mail do Destinatário;
    d. Domínio do Remetente;
    e. Domínio do Destinatário;
    f. Assunto da mensagem;
    g. Nome do anexo;
    h. Palavra contida no conteúdo do corpo da mensagem;
    i. IP de Origem da mensagem;
    j. Tamanho da mensagem;
    k. Nome da assinatura que gerou pontuação de SPAM no email;
    l. Regra de DLP;
    m. Se a mensagem foi entregue ou não;
    n. Regras personalizadas aplicadas na mensagem;
    o. Nome da ameaça encontrada; .Sentido da mensagem:
        .Entrada (De fora para dentro da empresa/órgão);

.Saída (De dentro para fora da empresa/órgão);
.Interna (De uma caixa postal para outra da mesma empresa/órgão);
.Todos (Entrada, Saída e Internos);

p. Por Pontuação da mensagem:
.Maior;
.Maior igual;
.Igual;
.Menor igual;
.Menor;

147. A console deve apresentar ainda as seguintes características de rastreamento de mensagens:
a. 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, conteúdo do corpo da mensagem, data, status, hora de entrega da mensagem, permitindo a concatenação dos filtros através dos operadores lógicos “e” e “ou”;
b. O rastreamento deve ser a partir de uma única interface de gerenciamento independente de qual equipamento que filtrou a mensagem, não sendo aceito pesquisa via linha de comando;
c. 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;
d. Deve apresentar como resultado as seguintes informações:
a.Remetente da mensagem;
b. Destinatários da mensagem;
c. Se foi armazenada em quarentena;

• Indicação de qual quarentena aplicada;

d. Se continha vírus;
e. As assinaturas que pontuaram;
f. IP de Origem;
g. O tamanho da mensagem;
h. Se foi entregue ou não;
i. Qual ponto de filtragem utilizado (por qual equipamento processou a mensagem).

e. No caso de a mensagem ter sido entregue, deve ser possível a apresentação do log de entrega da mesma e para qual IP entregue;
f. Se o e-mail tiver sido bloqueado por ser considerado spam ou possível spam, o log deve apresentar os filtros aplicados, bem como a pontuação apresentada por cada filtro e explicação do que representa o filtro aplicado (para facilidade do entendimento do administrador);
g. Deve ser capaz de visualizar a fila de e-mails em tempo real, bem como o sentido do e-mail na fila (se é fila de entrada ou saída), indicando total de e-mails na fila de saída, total de e-mails na fila de entrada e total de e-mails com erros na entrega;
h. Rastrear e-mails a partir de uma determinada ameaça;
i. Apresentar na interface gráfica as fontes de ataque e, através delas, apresentar quais e-mails foram recebidos, originários dessa fonte de ataque.

Da proteção contra SPAM e PHISHING

148. 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;
149. Permitir ao administrador definir filtros por URL através de categorias, divididas por assunto, sendo possível definir uma pontuação. Categorias mínimas contidas na solução:
a. Conteúdo pornográfico;
b. Abuso infantil;
c. Redes sociais;
d. Racismo e ódio;
e. Pesquisa de empregos;
f. Streaming de áudio;
g. Streaming de vídeo;
h. Esportes;
i. Notícias;
j. Compras Online.
150. Deve permitir que o administrador da solução possa recategorizar URL diretamente na interface gráfica da solução (sem necessidade de abrir sites de reclassificação);
151. 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;
152. 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;
153. Deve permitir que o administrador cadastre novas RBL’s a serem utilizadas a nível de cálculo de SPAM. O administrador deverá ter a autonomia para selecionar quais RBL’s serão utilizadas a nível de conexão SMTP e quais serão utilizadas a nível de cálculo de SPAM;
154. 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. Checagem de validade de domínio através de verificação da configuração da zona do DNS do remetente;
g. Análise de reputação de IP;

h. Reputação de Mensagens;
i. Filtros de URL;
j. Filtro de anti-phishing;
k. Consulta de RBL´s (real-time blackhole list);
l. Machine Learning.

155. 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, inclusive de outros fabricantes, não sendo restrito ao fluxo de mensagens do ambiente instalado, nem tão pouco somente em redes instaladas do próprio fabricante;
156. 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.
157. Possuir mecanismo de análise de conteúdo HTML no corpo da mensagem, permitindo ao administrador desarmar as tags HTML possivelmente perigosas e bloquear as mensagens, possuindo no mínimo a identificação das seguintes Tags:
    a. “<form>”;
    b. “<script>”;
    c. “<iframe>”.
158. 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.
159. 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;
160. 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;
161. A solução deve 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;
162. A Solução deve possuir de forma integrada a capacidade de coletar e analisar reports de dados de DMARC (relatórios padrão XML), sem necessidade de uso de ferramenta de terceiros;
163. O sistema de análise de relatórios de DMARC padrão XML (tanto o do tipo RUA – DMARC Aggregate Reporting, quanto do tipo RUF – DMARC Forensic Report), deve coletar as informações através de uma caixa postal dedicada aos relatórios de DMARC, através do protocolo POP ou IMAP;
164. Deve possuir dashboard apresentando os seguintes dados de DMARC à partir dos relatórios XMLs do tipo RUA (DMARC Aggregate Reporting). Essa função deve ser nativa na solução, não sendo aceita solução de terceiros integrada a ferramenta. O Dashboard deve apresentar no mínimo os seguintes dados:
    a. Indicação de falha e sucesso de DMARC;
    b. Indicação de falha e sucesso de DKIM (alinhamento de DKIM);
    c. Indicação de falha e sucesso de SPF (alinhamento de SPF);
    d. Quantidade de mensagens recebidas por dia, com indicação de falha ou sucesso na verificação de DMARC;
    e. Quantidade de mensagens analisadas agrupadas por domínio;
    f. Top 10 de IPs de origem dos e-mails reportados, com indicação de país de origem;
    g. Indicação de geolocalização de origem dos e-mails reportados;
165. A solução deve ter a capacidade de analisar os relatórios XMLs de DMARC do tipo RUF (DMARC Forensic Report), coletados à partir de uma caixa postal e efetuar análise e apresentação dos dados do mesmo em forma de dashboard, com tabelas e gráficos com indicadores de qualidade. Essa função deve ser nativa na solução, não sendo aceita solução de terceiros integrada a ferramenta;
166. 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;
167. Deve ter a capacidade de rejeitar mensagens para destinatários inválidos durante o diálogo SMTP (tratar Non-Delivery Report Attack);
168. Deve possuir proteção contra bounce e-mail attack através do método “Bounce Address Tag Verification”;
169. Deve permitir a inclusão de múltiplas listas de remetentes bloqueados, permitindo regras de bloqueio se o IP estiver presente nestas listas;
170. 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;
171. Deve possuir a capacidade de coleta dos relatórios XML de DMARC, do tipo RUA (DMARC Aggregate Reporting) e RUF (DMARC Forensic Report) através de uma caixa postal utilizando o protocolo POP3 ou IMAP;
172. Deve possuir sistema de análise de relatórios DMARC, coletando os relatórios XML do tipo RUA (DMARC Aggregate Reporting) e RUF (DMARC Forensic Report) gerando tabelas e gráficos referentes a esses relatórios, bem detecção de IP de Origem que causem falhas de alinhamento de DKIM e alinhamento de SPF, com uso do domínio da empresa/órgão;

173. A solução deve possuir dashboard de DMARC do tipo RUF (DMARC Forensic Report) e o mesmo deve possibilitar a pesquisa por IP de Origem, Assunto do Email, Headers Originais da mensagem, bem como verificar o conteúdo reportado (permitir ao administrador da ferramenta, caso tenha permissão de visualização de conteúdo, possibilitar visualizar o corpo da mensagem e URLs reportadas) no relatório XML;
174. 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:
    a. Microsoft Exchange;
175. Deve possuir sistema de reconhecimento de imagens pornográficas, cobrindo no mínimo os seguintes parâmetros:
    a. Percentual de cobertura de cor de pele na imagem, para que a imagem seja considerada nudez ou pornográfica;
    b. Tamanho da imagem a ser analisada (área de cobertura da cor de pele em relação ao tamanho total da imagem);
    c. Curvatura do corpo;
    d. Comparação da imagem com o fundo;
    e. Comparação da imagem com o contexto do email;

Da proteção contra VÍRUS e malwares

176. Possuir módulo de verificação com suporte a dois ou mais mecanismos diferentes de antivírus, executando simultaneamente, sendo um deles do próprio fabricante da solução;
177. Deverá ser capaz de filtrar vírus nos dois sentidos de tráfego (entrada e saída de email);
178. Scan de arquivos compactados recursivamente, no mínimo, 5 (cinco) camadas, contemplando no mínimo, os seguintes compactadores: .RAR, .ZIP, .TAR, .ARJ, .CAB, .LHA, .ACE, .LZH, .TGZ, .GZIP, .BZIP, .7Z, .TZH, .TGZ;
179. A solução deve possuir, no mínimo, duas engines de antivírus e antimalware já integrados na solução sem custo adicional;
180. Deve possuir sistema de detecção a técnicas de mascaramento de ameaças, sendo de no mínimo dos seguintes tipos de ataque:
    a. Stealth;
    b. Ameaças polimórficas;
    c. Técnicas de esteganografia;
181. 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.
182. Deve possuir capacidade de extrair senhas no corpo do email e adicionar a um banco de senhas, para posteriormente ser utilizado para descriptografar anexos compactados com senha;
183. Deve possuir um banco de senhas, ao qual permite ao administrador adicionar e remover senhas a serem utilizadas para descriptografar anexos compactados com senha;

Das notificações de quarentena individual do usuário

184. A solução deverá permitir ao administrador agendar o envio do resumo das mensagens na quarentena individual do usuário (digest) em períodos de tempo préconfiguráveis 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;
185. Grupos diferentes de usuários devem poder receber a notificação em horários diferentes;
186. 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; 187. 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;
188. 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 do mesmo 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. Solicitar envio de novo resumo;
    f. Acessar sua área de quarentena;
189. 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 (VÍRUS);
190. A solução deverá permitir ao administrador selecionar quais ações serão liberadas para o usuário final selecionar, no mínimo:
    • Liberar e-mail;
    • Reportar;
    • Incluir o remetente do e-mail em blacklist individual (do próprio usuário);
    • Incluir o remetente do e-mail em whitelist individual (do próprio usuário);
    • Visualizar o e-mail;
191. Deve disponibilizar manual específico para uso da quarentena individual (digest) para os usuários finais (independente do manual do administrador do sistema), na língua portuguesa do Brasil em formato editável, dessa forma o órgão poderá utilizar o mesmo para distribuir aos seus usuários finais, com o mínimo de alteração;

Do disclaimer

192. Capacidade de incluir “disclaimers” nas mensagens enviadas;
193. A solução deverá suportar aplicação de “disclaimers” diferenciados para usuários e grupos diferentes através da integração com o serviço de diretório LDAP ou Microsoft Active Directoy;
194. A solução deverá suportar a configuração dos “disclaimers” em formato html e texto;
195. A solução deve permitir a inclusão do “disclaimer” no começo ou no final do email, permitindo ao administrador selecionar onde desejar;

Prevenção a roubo de informação (DLP) e Compliance

196. 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;
197. 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;
198. 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. Também deve possuir dicionários de expressões

regulares já existentes na ferramenta, dentre eles:

a. Identificação de CPF;
b. Número de cartão de crédito;
c. Número do passaporte brasileiro;
d. CNH (Carteira Nacional de Habilitação);
e. RG;
f. Placa de carro padrão Mercosul;
g. CNPJ.

199. 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:
    a. Cabeçalho;
    b. URL (contidas no e-mail);
    c. Corpo do e-mail;
    d. Anexos e documentos no mínimo: .DOC, .DOCX, .XLS, .XLSX, .PDF, .PPT, .PPTX e .TXT.
200. 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;
201. Todos os itens do DLP devem permitir configurações através de regras que permitam ao administrador definir, no mínimo, as seguintes ações:
    a. Entregar a mensagem;
    b. Não entregar a mensagem;
    c. Armazenar a mensagem para auditoria;
    d. Notificar remetente e destinatário da mensagem;
    e. Encaminhar a mensagem para outro destinatário.
202. Todos os itens do DLP devem permitir configurações que permitam ao administrador criar regras complexas através de operadores lógicos “E” e “OU”;
203. 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;
204. Possibilitar ao administrador integrar o DLP com a criptografia, de modo a que os emails sigilosos somente sejam enviados criptografados;

Criptografia de E-mail

205. 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;
206. 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 customizável pelo administrador;
207. A console de gerenciamento do módulo de criptografia deve ser a mesma para toda a solução, não exigindo console de administração adicional;
208. Deve possibilitar ao administrador, definir quais mensagens serão criptografadas com base no mínimo em:
    a. Assunto;
    b. Destinatário;
    c. E-mail do Remetente;
    d. Nome do Anexo;
    e. Cabeçalho específico no email;
209. A criptografia das mensagens deve utilizar sistema de chaves gerada de forma independente;
210. Deve permitir efetuar a criptografia automática de email, mediante tolken contido no email;
211. Deve impossibilitar o uso de Cache de Browser para acesso as mensagens criptografadas;
212. Deve possibilitar ao administrador a indicação do tempo de expiração da mensagem criptografada;
213. Deve possibilitar ao administrador indicar se o destinatário poderá responder o email;
214. Deve possibilitar ao administrador indicar se o destinatário poderá encaminhar o email.
215. A solução de criptografia de emails deve ser responsivo, permitindo aos usuários lerem emails criptografados na solução tanto em tablets, como em celulares smartphones, incluindo iPhones.

Do Sistema de Proteção Contra Ataques Dirigidos (Targeted Attack Protection - TAP)

216. Deverá prover proteção contra ataques dirigidos tais como:
    a. Spear-phishing;
    b. Ataques Zero-Day;
    c. Ameaças avançadas persistentes (APTs).
217. Deve possuir técnica para construção de modelos estatísticos com Big Data; 218. Deve possuir no mínimo 3 (três) camadas de proteção sendo elas:
    a. Verificação da lista de códigos maliciosos: Verificação de campanhas de e-mails emergentes e conhecimento de novos sites maliciosos;
    b. Análise Estática (Análise de código): Verificação de comportamento suspeito, scripts escondidos, partes de códigos maliciosos e redirecionamento a outros sites maliciosos;
    c. Análise Dinâmica: Utilização de “Sandbox” para simular a máquina de um usuário real e observar as alterações efetuadas no sistema.
219. Possuir, dentro da solução, um dashboard do módulo de Segurança contra-ataques dirigidos;
220. O sistema de proteção contra-ataques dirigidos deve executar no mínimo 3 (três) etapas:
    a. 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;
    b. Proteção - Deve assegurar que links para URLs sejam 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;
    c. 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.
221. Não será aceita solução baseada apenas em reputação de URL;
222. A solução deve conter engine para detecção de Anomalias, não podendo se limitar a analise com definições baseadas em ataques já conhecidos;
223. Deve ser possível habilitar ou desabilitar a proteção URL baseada em rotas especificas configuradas no mínimo pelas seguintes condições:
    a. E-mail do Destinatário;
    b. E-mail do Remetente;
    c. Domínio de Origem;
    d. Domínio de Destino;
    e. IP/Rede;
    f. Range de IP;

g. Expressão Regular;
h. Usuários;
i. Listas de distribuição;
j. Grupo de LDAP.

224. 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 mensagem de alerta e o site deverá ser bloqueado para acesso;
225. O sistema deverá ser capaz de varrer anexos, com no mínimo, tipos PDF, arquivos em Flash para payloads maliciosos e microsoft office;
226. Ao detectar arquivos maliciosos, deverá ser capaz de configurar regras para bloquear o email contaminado e higienizar o anexo;
227. Deve possuir tecnologia de SandBox do mesmo fabricante, 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) ou ter a capacidade de instalação de SandBox local com todas as regras da legislação vigente brasileira (Lei Geral de Proteção de Dados Pessoais);
228. 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 “Analise Comportamental” do arquivo identificando assim malwares e variantes sem a necessidade de assinaturas;
229. O sistema de SandBox em nuvem do fabricante, deve ter a capacidade de suportar análise de no mínimo 50.000 arquivos ao mês;
230. O SandBox deve ser local ou em nuvem do fabricante. Sendo em nuvem do fabricante, deve estar localizado fisicamente no Brasil ou no mínimo conter nodes que compõem o cluster do SandBox em datacenter no Brasil, obedecendo a instrução normativa nº5 de 30 de agosto de 2021 da legislação brasileira, o(s) datacenter(s) deve(m) estar localizado(s) no Brasil;
231. 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;
232. A proteção URL deverá reescrever links para os protocolos HTTP, HTTPS, FTP e URL's que comecem com “www” independente do protocolo;
233. 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;
234. A solução deverá prover lista de exceções de URL para que não sejam reescritas;
235. O Dashboard deverá exibir o número de cliques em cada ameaça;
236. O Dashboard deverá exibir qual usuário clicou na URL detectada como ameaça;
237. 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 ameaças no mínimo com as seguintes informações:
    a. 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;
    b. Bloqueado - Número de vezes que o modulo de Proteção URL impediu o usuário de acessar o site malicioso;
    c. 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.
238. O Dashboard deverá exibir timeline das ameaças, exibindo quando foi recebida, identificada e quando foi clicada ou liberada;
239. No Dashboard deverá ser possível filtrar uma URL em um campo de busca para analisar todas as ocorrências com aquela URL, bem como verificar o status atual dela e preview da página web;
240. O Dashboard deverá possuir ferramenta para bloqueio ou liberação de URL pelo administrador da ferramenta;
241. No Dashboard deverá ser possível filtrar um IP em um campo de busca para analisar todas as ocorrências com aquele IP, bem como verificar o status atual dele e preview da página web;
242. O Dashboard deverá disponibilizar sistema de coleta (report) de amostra do IP para análise da engenharia do fabricante;
243. O Dashboard deverá possuir ferramenta para bloqueio ou liberação do IP pelo administrador da ferramenta;
244. No Dashboard deverá ser possível ao administrador enviar uma amostra de um arquivo para análise e visualizar o retorno de todas as ocorrências encontradas para esse arquivo;
245. O Dashboard deverá possuir ferramenta para bloqueio ou liberação do arquivo pelo administrador da ferramenta;
246. A ferramenta de segurança contra ataques dirigidos, deve possuir o sistema colaborativo, ao qual o administrador poderá configurar que o usuário final possa indicar liberação e bloqueio de URL’s, mesmo analisados pelo sistema e dessa forma reportando falsos positivos e falsos negativos. Deve prover também um Dashboard onde o Administrador poderá verificar todos reports enviados pelos usuários, ficando a cargo do administrador decidir pelo bloqueio ou a liberação de tal URL e/ou Arquivo;
247. Deve possuir módulo de CDR “Content Disarm and Reconstruction”, que quando ativado irá remover conteúdos possivelmente perigosos, em no mínimo para os seguintes tipos:
    a. JavaScript;
    b. Links;
    c. Executáveis;
    d. VB Script.

    De dentro de documentos, em no mínimo para os seguintes tipos:
    a. pdf;
    b. doc;
    c. docx;
    d. ppt;
    e. pptx;
    f. xls;
    g. xlsx.
248. Deve possuir capacidade de ignorar reescrita de algumas URL’s e não envio de arquivos para análise no SandBox do fabricante;
249. O SandBox do fabricante deve ter a capacidade de analisar arquivos, mesmo que estejam inseridos em arquivos compactados, do tipo:
    a. .swf;
    b. .pdf;
    c. .doc;
    d. .xls;
    e. .xlsx;
    f. .ppt;
    g. .ppt;
    h. .pptx;
    i. .rtf.
250. Deve ter a opção de não fazer reescrita de URL’s em casos de mensagens oriundas de determinados países, por exemplo: Mensagens oriundas da

China, Austrália e Belize;

251. Deve poder desativar a reescrita de URL's se a mensagem atingir uma pontuação mínima de SPAM definida pelo administrador;
252. Possibilidade do administrador de incluir URL's, arquivos e IP's em uma lista de bloqueio (Blacklist) no sistema de detecção;
253. Possibilidade do administrador de incluir URL's, arquivos e IP's em uma lista segura (Whitelist) no sistema de detecção;
254. Deve permitir rastrear todos os emails envolvidos (que contenham a mesma URL) à partir da URL afetada pelo módulo de Proteção Contra Ataques Dirigidos;

Do Sistema de Proteção a Fraudes de E-mail

255. A solução deverá ter a capacidade de detectar domínios recém registrados (tempo considerado como recém adquirido deverá ser configurável pelo administrador) e indicar o que deve ser feito neste caso:
    a. Pontuar;
    b. Ignorar;
    c. Bloquear.
256. 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:
    a. Pontuar;
    b. Ignorar;
    c. Bloquear.
257. 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;
258. Deve possuir sistema de detecção de e-mails oriundos de servidores de e-mails gratuitos (sem necessidade de cadastro manual dos IP's dos mesmos) tais como Google, Yahoo, Hotmail, etc, e o remetente dos emails dessas fontes tiver sido forjado, possibilitar efetuar as seguintes ações:
    a. Pontuar;
    b. Ignorar;
    c. Bloquear.
259. 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;
260. Deve possuir sistema de detecção e prevenção de ataques com TLD (Top Level Domain);
261. Deve ter a capacidade de cadastro e comparação de "Display Name", para proteção contra emails forjados;

Archiving e Auditoria de Email

262. O sistema de Auditoria/Archiving, deverá possuir interface de gerenciamento web via HTTPS, ao qual será possível administrar também toda a solução;
263. Será permitido soluções de gerenciamento unificadas com a "Solução de Segurança Anti-Spam e E-mail Gateway" OU soluções de terceiros desde que devidamente licenciadas e passíveis de integração com a "Solução de Segurança Anti-Spam e E-mail Gateway" e com o sistema de correio Eletrônico Microsoft Exchange;
264. O sistema deve permitir o armazenamento e todas as mensagens Entrada/Saída da corporação, bem como ter a capacidade de armazenar os e-mails internos trafegados dentro da empresa (desde que as mesmas passem pelo sistema de Email Gateway);
265. Deve permitir a integração com sistema de correio Microsoft Exchange para o armazenamento dos e-mails internos do domínio. Esta integração pode ser feita através de uma conta especifica no Microsoft Exchange usando o protocolo POP3 ou através do uso de conectores para o envio e recebimento das mensagens utilizando protocolo SMTP/TLS;
266. A solução deve permitir integração com a "Solução de Segurança Anti-Spam e E-mail Gateway" através do protocolo SMTP/TLS para armazenamento das mensagens, OU caso a solução seja do mesmo fabricante será permitido integração através protocolo proprietário da solução;
267. O sistema deve permitir que o administrador configure o tempo de armazenamento e o "rotacionamento" automático das mensagens utilizando pelo menos os seguintes critérios:
    a. Por número x de dias;
    b. Por número x de meses;
    c. Por número x de anos;
    d. E/OU volume de armazenamento de dados em MB/GB;
268. O sistema deve ter a capacidade de dimensionado para permitir o armazenamento de todas as mensagens por um período mínimo de 5 anos;
269. O sistema deve garantir acesso criptografado as mensagens armazenadas, evitando o acesso não autorizado aos arquivos e ao conteúdo dos e-mails armazenados, assim aumentando a confiabilidade e segurança da solução;
270. Deve ser possível criar usuários específicos para Auditoria/Archiving com permissões distintas a fim de limitar o acesso às informações, desta forma a solução deverá possuir no mínimo os seguintes perfis de acesso:
    a. Permitir definir o Domínio/Email que um usuário pode ter acesso;
    b. Definir se o usuário deverá ou não ter acesso ao conteúdo da mensagem/anexos;
    c. Permitir a criação de usuários para administração da ferramenta de forma granular, ou seja, definir quais áreas do sistema o usuário poderá ter acesso;
271. O sistema deve permitir criar usuário do tipo Auditor que tenha permissão de visualizar através da interface web os e-mails que forem colocados para auditoria e/ou efetuados archiving, sendo possível definir quais endereços de e-mails ou domínios ele poderá auditar;
272. O recurso de archiving e/ou auditoria deve permitir a integração ao módulo de DLP, para que caso seja disparada alguma regra de DLP, o mesmo possa armazenar os registros do email no sistema de Archiving e/ou Auditoria;
273. A solução deve permitir o armazenamento das mensagens em disco Interno da solução e também possibilitar a integração com sistemas de armazenamentos externos para expansão, sendo compatível com pelo menos um dos seguintes tipos: HBA, Fibre Channel, iSCSI ou Storage Externo NAS;
274. O sistema deve permitir a consulta de emails em:
    a. Emails circulados na solução;
    b. Archiving;
    c. Emails auditados;

    Para a busca nesses módulos, deve permitir busca pelos seguintes campos:

    a. ID da mensagem;
    b. IP de Origem da mensagem;
    c. Assunto do email;
    d. DE;
    e. PARA;
    f. Palavras contidas no corpo da mensagem;
    g. Nome de anexo;
    h. Tamanho da mensagem;

i. Data;

275. A solução deve permitir a realização de backup dos dados para um sistema de backup externo. Serão aceitas soluções que permitam exportar os dados para um compartilhamento externo ou que permitam a instalação de agente de backup;
276. O sistema deve permitir auditoria completa das mensagens incluindo a possibilidade do Download da mensagem Original e/ou seus anexos;
277. Ser compatível com as principais normas de segurança da informação tais como: LGPD e SOX;
278. Permitir auditoria completa das ações realizadas por qualquer pessoa que tenha acessado a solução através da interface Web), com no mínimo registro das seguintes informações:
    - Data e hora da ação;
    - Usuário que fez a ação;
    - Ação executada;
    - IP de quem fez a ação;
279. O sistema de auditoria deve apresentar a indicação de criação e/ou remoção de whitelist e blacklist. Caso seja um evento de remoção de whitelist ou blacklist, apresentar os dados anteriores a remoção da whitelist ou blacklist, para que o administrador possa recriar o registro se necessário.
280. Possibilitar o encaminhamento (envio) da Mensagem armazenada;
281. Permitir integração com os Serviços de Diretórios para acesso a solução: Microsoft AD, LDAP;
282. Possibilidade de gerar relatórios dos e-mails Armazenados para Archiving/Auditoria com as seguintes opções:
    a. Data;
    b. Origem/Destino;
    c. Domínio;

Integração com Microsoft 365

283. Possuir integração com a solução ao Microsoft Office 365 através de API, dessa forma, permitindo que o administrador realize diversas ações sobre a caixa de email do usuário final (diretamente pela interface gráfica da solução, sem necessidade de inclusão de módulos extras ou software de terceiros), entre eles:
    - Remoção de Anexos nos emails já entregues ao servidor de email;
    - Remoção de links em emails já entregues ao servidor de email;
    - Mover o email entregue ao servidor de email para a lixeira eletrônica;
    - Bloqueio de conteúdo de mensagem entregue ao servidor de email;
    - Apagar da caixa de correio eletrônico do usuário, uma ou mais mensagens já entregues ao servidor de email;
284. Possuir Plugin 'AddOn' compatível com Office 365 e com Outlook Desktop que permita adicionar um botão de ação visível para todos os usuários dentro de sua caixa de correio que permita as seguintes ações nas mensagens do usuário:
    a. Aprender Mensagem como SPAM e Não SPAM
    b. Enviar amostra de Phishing, Vírus ou outra ameaça ao administrador, contendo uma cópia do email original para que o administrador possa analisar e tomar as devidas providencias
285. Possuir Plugin 'AddOn' compatível com Office365 e com Outlook Desktop que permita adicionar um botão de ação visível para todos os usuários dentro de sua caixa de correio que permita ao usuário visualizar sua quarentena de emails que estão retidas na solução de Antispam, de forma integrada sem necessidade de acesso a outra ferramenta, com as seguintes ações:
    a. Permitir visualizar a quarentena de SPAM podendo o usuário liberar as mensagens que forem Falso Positivo;
    b. Permitir realizar pesquisa pelo Remetente e assunto do email de todos emails que ficaram retidos na quarentena da solução de Antispam
286. Possuir Plugin 'AddOn' compatível com Office365 e com Outlook Desktop que permita adicionar um botão de ação visível para todos os usuários dentro de sua caixa de correio que permita ao usuário visualizar sua lista de remetentes confiáveis e não confiáveis, de forma integrada sem necessidade de acesso a outra ferramenta, com as seguintes ações:
    a. Remoção de remetentes presentes na lista de confiáveis;
    b. Remoção de remetentes presentes na lista de não confiáveis;

Da manutenção e abertura de chamado técnico

287. O sistema deverá ter a capacidade de envio de estatísticas de performance ao fabricante (habilitado pelo administrador), para avaliação do mesmo para detecção e prevenção de excesso de consumo de disco, processamento e memória, prevenindo dessa forma interrupções e falhas por falta de recursos.
288. A contratada deve garantir para a **CONTRATANTE** o fornecimento de acesso irrestrito (24 horas x 7 dias da semana) à área de suporte do fabricante, especialmente ao endereço eletrônico (web site), a toda a documentação técnica pertinente (guias de instalação/configuração atualizados, FAQ's, bases de conhecimento e bases de soluções, com pesquisa efetuada através de ferramentas de busca).
289. A contratada deve apresentar o manual de administração da solução ofertada, na língua portuguesa (português do Brasil).
290. As respostas do suporte técnico contratado deverão ser efetuadas na língua portuguesa (português do Brasil), tanto por email, quanto por contato telefônico;
291. Caso seja necessário contato direto com o fabricante, o mesmo deve estar disponível para atendimento através de telefone disponibilizado pelo mesmo (no site, manual ou folders), em horário comercial (das 8:00h às 18:00h – horário de Brasília) e respondida em língua portuguesa (português do Brasil);
292. O suporte técnico deverá ser prestado em caso de falhas, dúvidas e/ou esclarecimentos de qualquer um dos produtos, módulos e programas referentes aos componentes da solução.
293. A abertura de chamados pelo **CONTRATANTE** será efetuada por correio eletrônico, por sistema de controle de chamados, com email de resposta do chamado aberto apresentando o número do ticket aberto, para acompanhamento.
294. O FABRICANTE DA SOLUÇÃO deverá fornecer os níveis de atendimento conforme abaixo indicado, com atendimento em língua portuguesa do Brasil (tanto por email, quanto por telefone e sistema de suporte técnico – service desk):
    - Os chamados de severidade ALTA (Quando há indisponibilidade de uso da solução) deverão ser atendidos em até 1 (uma) hora após a abertura e deverão ser solucionados em até 24 (vinte e quatro) horas, contados a partir da abertura do chamado.
    - Os chamados de severidade MÉDIA (Quando há falha, simultânea ou não, de uma ou mais funcionalidades que não cause indisponibilidade, mas apresente problemas de funcionamento e/ou performance da solução) deverão ser atendidos em até 4 (quatro) horas após a abertura e deverão ser solucionados em até 48 (quarenta e oito) horas, contados a partir da abertura do chamado.
    - Os chamados de severidade BAIXA (Nível de severidade aplicado para instalação, configuração, atualização de versões e implementações de novas funcionalidades) deverão ser atendidos em até 8 (oito) horas após a abertura e deverão ser solucionados em até 72 (setenta e duas) horas, contados a partir da abertura do chamado.
    - Os chamados de severidade INFORMATIVO (Nível informacional ou dúvidas) deverão ser atendidos em até 16 (dezesseis) horas após a abertura.
295. A **CONTRATADA** deverá possuir técnico especializado na solução, com no mínimo 1 (um) técnico certificado pelo fabricante e com certificação dentro da validade.

Da qualificação técnica da proponente

296. A proponente deverá apresentar atestado(s) de capacidade técnica, fornecido(s) por pessoa jurídica de direito público ou privado, comprovando que a licitante forneceu equipamentos e/ou softwares e prestou serviços de mesma natureza e compatíveis em características com o objeto, atestando,

inclusive, o bom desempenho e cumprimento a contento das obrigações contratuais.

297. Os atestados poderão ser objetos de diligência a fim de se esclarecer quaisquer dúvidas quanto ao seu conteúdo, inclusive com solicitação dos respectivos contratos que lhe deram origem, visitas ao local, etc.
298. No caso de a licitante não ser a fabricante dos equipamentos, não será permitida a apresentação de atestado de capacidade técnica do fabricante.
299. Todos os itens referentes a funcionalidades do produto deverão ser obrigatoriamente comprovados através de catálogos, manuais e/ou website oficial do fabricante juntamente com uma planilha de apontamentos contendo a indicação de documento e página correspondente a cada item da seção Especificações Técnicas deste Edital.
300. Estes documentos devem ser enviados pela proponente classificada em primeiro lugar juntamente com sua proposta comercial e tem o objetivo de garantir seu pleno atendimento ao instrumento convocatório. O não envio destes implica em desclassificação.

Treinamento

301. Deverá ser fornecido treinamento de capacitação técnica **OFICIAL DO FABRICANTE** da solução adquirida, sobre todos os aspectos de instalação, configuração, administração e suporte da solução de segurança de e-mails (AntiSpam).
302. O treinamento deverá ser remoto via EAD, ministrado no período acordado pelas partes, na cidade de Salvador, para uma turma de 05 participantes.
303. O modelo possui dois modos de treinamento oficial do fabricante –Remoto, de acordo com a necessidade do órgão:
    a. O treinamento da solução deverá ser o treinamento **OFICIAL DO FABRICANTE** (não sendo aceito treinamento com material montado de terceiros, nem utilização de material não homologado pelo fabricante da solução), sendo na forma remota, com no mínimo os seguintes requisitos:
        .O ambiente de treinamento remoto deve ser fornecido pela **CONTRATADA**, com todos os softwares, recursos e materiais didáticos necessários para o adequado aprendizado pelos participantes.
        .O treinamento deverá contemplar questões teóricas e práticas (hands-on), sobre o funcionamento da solução.
304. O treinamento deverá possuir carga horária mínima de 16 (dezesseis) horas, e será ministrado em dias úteis, em meio período (matutino ou vespertino) a ser escolhido pelo **CONTRATANTE**.

305. O conteúdo programático do curso deverá ser previamente aprovado pela **CONTRATANTE**. Eventuais modificações do conteúdo a ser ministrado, deverão ser aprovadas pelo **CONTRATANTE**, e deverá abranger todas as funcionalidades nativas da solução, assim como as customizáveis a serem implantadas.
306. A **CONTRATADA** deverá disponibilizar material didático oficial da fabricante da solução adquirida, sem custo adicional para a **CONTRATANTE**, para todos os participantes, no idioma português do Brasil. O início do curso ficará condicionado à disponibilização do material didático, em formato digital.
307. Deverá ser emitido certificado de participação a todos os participantes, contendo o conteúdo programático e a carga horária total, na conclusão do treinamento.

HSC DESENVOLVIMENTO E SERVIÇOS EM TECNOLOGIA DA INFORMAÇÃO LTDA
Romulo Giordani Boschetti
Cargo

MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA

André Luis Sant´Ana Ribeiro
Superintendente de Gestão Administrativa

(Assinado e datado eletronicamente/digitalmente)

Documento assinado eletronicamente por **ROMULO GIORDANI BOSCHETTI** - Usuário Externo, em 09/01/2025, às 11:35, conforme Ato Normativo n° 047, de 15 de Dezembro de 2020 - Ministério Público do Estado da Bahia.

Documento assinado eletronicamente por **André Luis Sant Ana Ribeiro** - Superintendente, em 09/01/2025, às 19:55, conforme Ato Normativo n° 047, de 15 de Dezembro de 2020 - Ministério Público do Estado da Bahia.

A autenticidade do documento pode ser conferida no site https://sei.sistemas.mpba.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1379600** e o código CRC **102C89D0**.