MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA
ARQUIVO NACIONAL

PREGÃO ELETRONICO Nº 10/2020

PROCESSO Nº 0008227.000024/2019-34

Torna-se público, para conhecimento dos interessados, que a União, por intermédio do Ministério da Justiça e Segurança Pública, representada pelo Arquivo Nacional, por meio do Pregoeiro designado pela Portaria nº 01, de 24 de julho de 2020, do Coordenador-Geral de Administração do Arquivo Nacional, publicada no D.O.U. nº 142, de 27 de Julho de 2020, sediado na Praça da República, nº 173 – Centro – Rio de Janeiro/RJ – CEP.: 20.211-350, realizará licitação, na modalidade PREGÃO, na forma ELETRÔNICA, **com o critério de julgamento menor preço global por GRUPO** sob a forma de execução indireta, no regime de empreitada por *preço global/integral)*, nos termos da Lei nº 10.520, de 17 de julho de 2002,da Lei nº 8.248, de 22 de outubro de 1991, do **Decreto nº 10.024, de 20 de setembro de 2019**, do Decreto 9.507, de 21 de setembro de 2018, do Decreto nº 7.746, de 05 de junho de 2012, **do Decreto nº 7.174, de 12 de maio de 2010**, da Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019, das Instruções Normativas SEGES/MP nº 05, de 26 de maio de 2017 e nº 03, de 26 de abril de 2018 e da Instrução Normativa SLTI/MPOG nº 01, de 19 de janeiro de 2010, da Lei Complementar n° 123, de 14 de dezembro de 2006, da Lei nº 11.488, de 15 de junho de 2007, do Decreto n° 8.538, de 06 de outubro de 2015, aplicando-se, subsidiariamente, a Lei nº 8.666, de 21 de junho de 1993 e as exigências estabelecidas neste Edital.

Data da sessão: 02/12/2020

Horário: 10:00 hs

Local: Portal de Compras do Governo Federal – www.comprasgovernamentais.gov.br

1. DO OBJETO

1.1 Aquisição de Solução de **Antivírus, Antispam,** para todo ambiente de rede do Arquivo Nacional – Ministério da Justiça e Segurança Pública, nas condições, quantidades e exigências estabelecidas neste Instrumento**,** conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

Grupo	Item	Descrição	Prazo de Garantia Contratual	Quantidade
I	1	Solução corporativa de Antivírus para estações de trabalho com gerência em nuvem	36 meses	650
	2	Solução corporativa de Antivírus para Servidores Físicos e Virtuais com gerência em nuvem.	36 meses	40

II	3	Solução de segurança anti-spam e e-mail gateway	12 meses	750

1.2 A licitação será dividida em grupos, formados por um ou mais itens, conforme tabela constante do Termo de Referência, facultando-se ao licitante a participação em quantos grupos forem de seu interesse, devendo oferecer proposta para todos os itens que os compõem.

1.3. *O critério de julgamento adotado será o* ***menor preço GLOBAL do Grupo,*** *observadas as exigências contidas neste Edital e seus Anexos quanto às especificações do objeto.*

1.4. *Cada serviço ou produto do lote deverá estar discriminado em itens separados nas propostas de preços, de modo a permitir a identificação do seu preço individual na composição do preço global, e a eventual incidência sobre cada item das margens de preferência para produtos e serviços que atendam às Normas Técnicas Brasileiras - NTB*

2. DOS RECURSOS ORÇAMENTÁRIOS

2.1 As despesas para atender a esta licitação estão programadas em dotação orçamentária própria, prevista no orçamento da União para o exercício de 2020, na classificação abaixo:

Gestão/Unidade: 200247
Fonte: 0144000000
Programa de Trabalho: 189988
Elemento de Despesa: 339040

PI: AN999LRTI20

3. DO CREDENCIAMENTO

3.1 O Credenciamento é o nível básico do registro cadastral no SICAF, que permite a participação dos interessados na modalidade licitatória Pregão, em sua forma eletrônica.

3.2 O cadastro no SICAF deverá ser feito no Portal de Compras do Governo Federal, no sítio www.comprasgovernamentais.gov.br, por meio de certificado digital conferido pela Infraestrutura de Chaves Públicas Brasileira – ICP - Brasil.

3.3 O credenciamento junto ao provedor do sistema implica a responsabilidade do licitante ou de seu representante legal e a presunção de sua capacidade técnica para realização das transações inerentes a este Pregão.

3.4 O licitante responsabiliza-se exclusiva e formalmente pelas transações efetuadas em seu nome, assumir como firmes e verdadeiras suas propostas e seus lances, inclusive os atos praticados diretamente ou por seu representante, excluída a responsabilidade do provedor do sistema ou do órgão ou entidade promotora da licitação por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros.

3.5 É de responsabilidade do cadastrado conferir a exatidão dos seus dados cadastrais no Sicaf e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados.

3.6 A não observância do disposto no subitem anterior poderá ensejar desclassificação no momento da habilitação.

4. DA PARTICIPAÇÃO NO PREGÃO.

4.1 Poderão participar deste Pregão interessados cujo ramo de atividade seja compatível com o objeto desta licitação, e que estejam com Credenciamento regular no Sistema de Cadastramento Unificado de Fornecedores – SICAF, conforme disposto no art. 9º da IN SEGES/MP nº 3, de 2018.

Os licitantes deverão utilizar o certificado digital para acesso ao Sistema

4.2 **Não poderão participar desta licitação os interessados:**

4.2.1 proibidos de participar de licitações e celebrar contratos administrativos, na forma da legislação vigente;

4.2.2 que não atendam às condições deste Edital e seu(s) anexo(s);

4.2.3 estrangeiros que não tenham representação legal no Brasil com poderes expressos para receber citação e responder administrativa ou judicialmente;

4.2.4 que se enquadrem nas vedações previstas no artigo 9º da Lei nº 8.666, de 1993;

4.2.5 que estejam sob falência, concurso de credores, concordata ou insolvência, em processo de dissolução ou liquidação;

4.2.6 entidades empresariais que estejam reunidas em consórcio;

4.2.7 organizações da Sociedade Civil de Interesse Público - OSCIP, atuando nessa condição (Acórdão nº 746/2014-TCU-Plenário);

4.2.8 instituições sem fins lucrativos (parágrafo único do art. 12 da Instrução Normativa/SEGES nº 05/2017)

> É admissível a participação de organizações sociais, qualificadas na forma dos arts. 5º a 7º da Lei 9.637/1998, desde que os serviços objeto desta licitação se insiram entre as atividades previstas no contrato de gestão firmado entre o Poder Público e a organização social (Acórdão nº 1.406/2017- TCU-Plenário), mediante apresentação do Contrato de Gestão e dos respectivos atos constitutivos.

4.2.9 sociedades *cooperativas, considerando a vedação contida no art. 10 da Instrução Normativa SEGES/MP nº 5, de 2017, bem como o disposto no Termo de Conciliação firmado entre o Ministério Público do Trabalho e a AGU..*

4.3 Nos termos do art. 5º do Decreto nº 9.507, de 2018, é vedada a contratação de pessoa jurídica na qual haja administrador ou sócio com poder de direção, familiar de:

a) detentor de cargo em comissão ou função de confiança que atue na área responsável pela demanda ou contratação; ou

b) de autoridade hierarquicamente superior no âmbito do órgão contratante.

4.3.1 Para os fins do disposto neste item, considera-se familiar o cônjuge, o companheiro ou o parente em linha reta ou colateral, por consanguinidade ou afinidade, até o terceiro grau (Súmula Vinculante/STF nº 13, art. 5º, inciso V, da Lei nº 12.813, de 16 de maio de 2013 e art. 2º, inciso III, do Decreto n.º 7.203, de 04 de junho de 2010);

4.4 Nos termos do art. 7° do Decreto n° 7.203, de 2010, é vedada, ainda, a utilização, na execução dos serviços contratados, de empregado da futura Contratada que seja familiar de agente público ocupante de cargo em comissão ou função de confiança neste órgão contratante.

4.5 Como condição para participação no Pregão, o licitante assinalará "sim" ou "não" em campo próprio do sistema eletrônico, relativo às seguintes declarações:

4.5.1 que cumpre os requisitos estabelecidos no artigo 3° da Lei Complementar nº 123, de 2006, estando apto a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49.

4.5.1.1 nos itens exclusivos para participação de microempresas e empresas de pequeno porte, a assinalação do campo "não" impedirá o prosseguimento no certame;

4.5.1.2 nos itens em que a participação não for exclusiva para microempresas e empresas de pequeno porte, a assinalação do campo "não" apenas produzirá o efeito de o licitante não ter direito ao tratamento favorecido previsto na Lei Complementar nº 123, de 2006, mesmo que microempresa, empresa de pequeno porte ou sociedade cooperativa.

4.5.2 que está ciente e concorda com as condições contidas no Edital e seus anexos;

4.5.3 que cumpre plenamente os requisitos de habilitação definidos no Edital e que a proposta apresentada está em conformidade com as exigências editalícias;

4.5.4 que inexistem fatos impeditivos para sua habilitação no certame, ciente da obrigatoriedade de declarar ocorrências posteriores;

4.5.5 que não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do artigo 7°, XXXIII, da Constituição;

4.5.6 que a proposta foi elaborada de forma independente, nos termos da Instrução Normativa SLTI/MP nº 2, de 16 de setembro de 2009.

4.5.7 que não possui, em sua cadeia produtiva, empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal;

4.5.8 que os serviços são prestados por empresas que comprovem cumprimento de reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social e que atendam às regras de acessibilidade previstas na legislação, conforme disposto no art. 93 da Lei nº 8.213, de 24 de julho de 1991.

4.5.9 que cumpre os requisitos do Decreto n. 7.174, de 2010, estando apto a usufruir dos critérios de preferência.

4.5.9.1 a assinalação do campo "não" apenas produzirá o efeito de o licitante não ter direito ao tratamento favorecido previsto no Decreto nº 7.174, de 2010.

4.6 A declaração falsa relativa ao cumprimento de qualquer condição sujeitará o licitante às sanções previstas em lei e neste Edital.

5 DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

5.1 Os licitantes encaminharão, exclusivamente por meio do sistema, concomitantemente com os documentos de habilitação exigidos no edital, proposta com a descrição do objeto ofertado e o preço, até a data e o horário estabelecidos para a abertura da sessão pública, quando, então, encerrar-se-á automaticamente a etapa de envio desse documento.

5.2 O Envio da proposta, acompanhada dos documentos de habilitação exigidos neste Edital, ocorrerá por meio de chave de acesso e senha.

5.3 Os licitantes poderão deixar de apresentar os documentos de habilitação que constem do SICAF, assegurado aos demais licitantes o direito de acesso aos dados constantes dos sistemas.

5.4 As Microempresas e Empresas de Pequeno Porte deverão encaminhar a documentação de habilitação, ainda que haja alguma restrição de regularidade fiscal e trabalhista, nos termos do art, 43, §1º, da LC nº 123, de 2006.

5.5 Incumbirá ao licitante acompanhar as operações no sistema eletrônico durante a sessão pública do Pregão, ficando responsável pelo ônus decorrente da perda de negócios, diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão.

5.6 Até a abertura da sessão pública, os licitantes poderão retirar ou substituir a proposta e os documentos de habilitação anteriormente inseridos no sistema;

5.7 Não será estabelecida, nessa etapa do certame, ordem de classificação entre as propostas apresentadas, o que somente ocorrerá após a realização dos procedimentos de negociação e julgamento da proposta.

5.8 Os documentos que compõem a proposta e a habilitação do licitante melhor classificado somente serão disponibilizados para avaliação do pregoeiro e para acesso público após o encerramento do envio de lances.

6 PREENCHIMENTO DA PROPOSTA

6.1 O licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, dos seguintes campos:

6.1.1 *Valor total Global do Grupo I e/ou do Grupo II*

6.1.2 Descrição do objeto, contendo as informações similares à especificação do Termo de Referência.

6.2 Todas as especificações do objeto contidas na proposta vinculam a Contratada.

6.3 Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na prestação dos serviços, apurados mediante o preenchimento do modelo de Planilha de Custos e Formação de Preços, conforme anexo deste Edital;

6.4 A Contratada deverá arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, tais como os valores providos com o quantitativo de vale transporte, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da licitação, exceto quando ocorrer algum dos eventos arrolados nos incisos do §1° do artigo 57 da Lei n° 8.666, de 1993.

6.5 Caso o eventual equívoco no dimensionamento dos quantitativos se revele superior às necessidades da contratante, a Administração deverá efetuar o pagamento seguindo estritamente as regras contratuais de faturamento dos serviços demandados e executados, concomitantemente com a realização, se necessário e cabível, de adequação contratual do quantitativo necessário, com base na alínea "b" do inciso I do art. 65 da Lei n. 8.666/93 e nos termos do art. 63, §2° da IN SEGES/MPDG n. 5/2017.

6.6 A empresa é a única responsável pela cotação correta dos encargos tributários. Em caso de erro ou cotação incompatível com o regime tributário a que se submete, serão adotadas as orientações a seguir:

6.7 cotação de percentual menor que o adequado: o percentual será mantido durante toda a execução contratual;

6.8 cotação de percentual maior que o adequado: o excesso será suprimido, unilateralmente, da planilha e haverá glosa, quando do pagamento, e/ou redução, quando da repactuação, para fins de total ressarcimento do débito.

6.9 Se o regime tributário da empresa implicar o recolhimento de tributos em percentuais variáveis, a cotação adequada será a que corresponde à média dos efetivos recolhimentos da empresa nos últimos doze meses, devendo o licitante ou contratada apresentar ao pregoeiro ou à fiscalização, a qualquer tempo, comprovação da adequação dos recolhimentos, para os fins do previsto no subitem anterior.

6.10 Independentemente do percentual de tributo inserido na planilha, no pagamento dos serviços, serão retidos na fonte os percentuais estabelecidos na legislação vigente.

6.11 A apresentação das propostas implica obrigatoriedade do cumprimento das disposições nelas contidas, em conformidade com o que dispõe o Termo de Referência, assumindo o proponente o compromisso de executar os serviços nos seus termos, bem como de fornecer os materiais, equipamentos, ferramentas e utensílios necessários, em quantidades e qualidades adequadas à perfeita execução contratual, promovendo, quando requerido, sua substituição.

6.12 Os preços ofertados, tanto na proposta inicial, quanto na etapa de lances, serão de exclusiva responsabilidade do licitante, não lhe assistindo o direito de pleitear qualquer alteração, sob alegação de erro, omissão ou qualquer outro pretexto.

6.13 O prazo de validade da proposta não será inferior a 60 (Sessenta) dias, a contar da data de sua apresentação.

6.14 Os licitantes devem respeitar os preços máximos estabelecidos nas normas de regência de contratações públicas federais, quando participarem de licitações públicas;

6.15 O descumprimento das regras supramencionadas pela Administração por parte dos contratados pode ensejar a responsabilização pelo Tribunal de Contas da União e, após o devido processo legal, gerar as seguintes consequências: assinatura de prazo para a adoção das medidas necessárias ao exato cumprimento da lei, nos termos do art. 71, inciso IX, da Constituição; ou condenação dos agentes públicos responsáveis e da empresa contratada ao pagamento dos prejuízos ao erário, caso verificada a ocorrência de superfaturamento por sobrepreço na execução do contrato

7 DA ABERTURA DA SESSÃO, CLASSIFICAÇÃO DAS PROPOSTAS E FORMULAÇÃO DE LANCES

7.1 A abertura da presente licitação dar-se-á em sessão pública, por meio de sistema eletrônico, na data, horário e local indicados neste Edital.

7.2 O Pregoeiro verificará as propostas apresentadas, desclassificando desde logo aquelas que não estejam em conformidade com os requisitos estabelecidos neste Edital, contenham vícios insanáveis, ilegalidades, ou não apresentem as especificações exigidas no Termo de Referência.

7.3 Também será desclassificada a proposta que **identifique o licitante.**

7.4 A desclassificação será sempre fundamentada e registrada no sistema, com acompanhamento em tempo real por todos os participantes.

7.5 A não desclassificação da proposta não impede o seu julgamento definitivo em sentido contrário, levado a efeito na fase de aceitação.

7.6 O sistema ordenará automaticamente as propostas classificadas, sendo que somente estas participarão da fase de lances.

7.7 O sistema disponibilizará campo próprio para troca de mensagens entre o Pregoeiro e os licitantes.

7.8 Iniciada a etapa competitiva, os licitantes deverão encaminhar lances exclusivamente por meio de sistema eletrônico, sendo imediatamente informados do seu recebimento e do valor consignado no registro.

7.9 *O lance deverá ser ofertado pelo valor total do lote (Grupo I) e Lote (Grupo II)*

7.10 Os licitantes poderão oferecer lances sucessivos, observando o horário fixado para abertura da sessão e as regras estabelecidas no Edital.

7.11 O licitante somente poderá oferecer lance de valor inferior ou percentual de desconto superior ao último por ele ofertado e registrado pelo sistema.

7.12 *O intervalo mínimo de diferença de valores ou percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser* **de 1% (um por cento).**

7.13 *Será adotado para o envio de lances no pregão eletrônico o* **modo de disputa "aberto e fechado",** *em que os licitantes apresentarão lances públicos e sucessivos, com lance final e fechado.*

7.14 *A etapa de lances da sessão pública terá duração inicial de quinze minutos. Após esse prazo, o sistema encaminhará aviso de fechamento iminente dos lances, após o que transcorrerá o período de tempo de até dez minutos, aleatoriamente determinado, findo o qual será automaticamente encerrada a recepção de lances.*

7.15 *Encerrado o prazo previsto no item anterior, o sistema abrirá oportunidade para que o autor da oferta de valor mais baixo e os das ofertas com preços até dez por cento superiores àquela possam ofertar um lance final e fechado em até cinco minutos, o que será sigiloso até o encerramento deste prazo.*

7.16 *Não havendo, pelo menos, três ofertas nas condições definidas neste item poderão os autores dos melhores lances subsequentes, na ordem de classificação, até o máximo de três, oferecer um lance final e fechado até cinco minutos, o qual será sigiloso até o encerramento deste prazo.*

7.17 *Após o término dos prazos estabelecidos nos itens anteriores, o sistema ordenará os lances segundo a ordem crescente de valores.*

7.18 *Não havendo lance final fechado e classificado na forma estabelecida nos itens anteriores, haverá o reinício da etapa fechada para que os demais licitantes, até no máximo de três, na ordem de classificação,* **possam ofertar um lance final e fechado em até cinco minutos**, *o qual será sigiloso até o encerramento deste prazo, observando-se, após, o item anterior.*

7.19 *Poderá o pregoeiro, auxiliado pela equipe de apoio, justificadamente, admitir o reinício da etapa fechada, caso nenhum licitante classificado na etapa de lance fechado atender as exigências de habilitação*

7.20 Não serão aceitos dois ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado em primeiro lugar.

7.21 Durante o transcurso da sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado, vedada a identificação do licitante.

7.22 No caso de desconexão com o Pregoeiro, no decorrer da etapa competitiva do Pregão, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances.

7.23 Quando a desconexão do sistema eletrônico para o pregoeiro persistir por tempos superior a dez minutos, a sessão pública será suspensa e reiniciada somente após decorridas vinte e quatro horas após a comunicação do fato aos participantes no sítio eletrônico utilizado para divulgação.

7.24 O Critério de julgamento adotado será o menor preço/maior desconto, conforme definido neste Edital e seus anexos.

7.25 Caso o licitante não apresente lances, concorrerá com o valor de sua proposta.

7.26 Em relação a itens não exclusivos para participação de microempresas e empresas de pequeno porte, uma vez encerrada a etapa de lances, será efetivada a verificação automática, junto à Receita Federal, do porte da entidade empresarial. O sistema identificará em coluna própria as microempresas e empresas de pequeno porte participantes, procedendo à comparação com os valores da primeira colocada, se esta for empresa de maior porte, assim como das demais classificadas, para o fim de aplicar-se o disposto nos arts. 44 e 45 da LC nº 123, de 2006, regulamentada pelo Decreto nº 8.538, de 2015.

7.27 Nessas condições, as propostas de microempresas e empresas de pequeno porte que se encontrarem na faixa de até 5% (cinco por cento) acima da melhor proposta ou melhor lance serão consideradas empatadas com a primeira colocada.

7.28 A melhor classificada nos termos do item anterior terá o direito de encaminhar uma última oferta para desempate, obrigatoriamente em valor inferior ao da primeira colocada, no prazo de 5 (cinco) minutos controlados pelo sistema, contados após a comunicação automática para tanto.

7.29 Caso a microempresa ou a empresa de pequeno porte melhor classificada desista ou não se manifeste no prazo estabelecido, serão convocadas as demais licitantes microempresa e empresa de pequeno porte que se encontrem naquele intervalo de 5% (cinco por cento), na ordem de classificação, para o exercício do mesmo direito, no prazo estabelecido no subitem anterior.

7.30 No caso de equivalência dos valores apresentados pelas microempresas e empresas de pequeno porte que se encontrem nos intervalos estabelecidos nos subitens anteriores, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta.

7.31 Só poderá haver empate entre propostas iguais (não seguidas de lances), ou entre lances finais da fase fechada do modo de disputa aberto e fechado.

7.32 Havendo eventual empate entre propostas ou lances, o critério de desempate será aquele previsto no art. 3º, § 2º, da Lei nº 8.666, de 1993, assegurando-se a preferência, sucessivamente, aos bens produzidos:

7.33 prestados por empresas brasileiras;

7.34 prestados por empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País;

7.35 prestados por empresas que comprovem cumprimento de reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social e que atendam às regras de acessibilidade previstas na legislação.

7.36 Persistindo o empate, a proposta vencedora será sorteada pelo sistema eletrônico dentre as propostas ou os lances empatados.

7.37 Encerrada a etapa de envio de lances da sessão pública, o pregoeiro deverá encaminhar, pelo sistema eletrônico, contraproposta ao licitante que tenha apresentado o melhor preço, para que seja obtida melhor proposta, vedada a negociação em condições diferentes das prevista deste Edital..

7.38 A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes.

7.39 O pregoeiro solicitará ao licitante melhor classificado que, no prazo de 02 (duas) horas envie a proposta adequada ao último lance ofertado após a negociação realizada, acompanhada, se for o caso, dos documentos complementares, quando necessários à confirmação daqueles exigidos neste Edital e já apresentados.

7.40 Após a negociação do preço, o Pregoeiro iniciará a fase de aceitação e julgamento da proposta.

7.41 Será assegurado o direito de preferência previsto no seu artigo 3º, conforme procedimento estabelecido nos artigos 5° e 8° do Decreto n° 7.174, de 2010.

7.42 As licitantes qualificadas como microempresas ou empresas de pequeno porte que fizerem jus ao direito de preferência previsto no Decreto nº 7.174, de 2010, terão prioridade no exercício desse benefício em relação às médias e às grandes empresas na mesma situação.

8 DA ACEITABILIDADE DA PROPOSTA VENCEDORA.

8.1 Encerrada a etapa de negociação, o pregoeiro examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade de preço em relação ao máximo estipulado para contratação neste Edital e em seus anexos, observado o disposto no parágrafo único do art. 7º e no §9º do art. 26 do Decreto nº 10.024/2019.

8.2 A análise da exequibilidade da proposta de preços deverá ser realizada de acordo com o Modelo de Proposta Comercial a ser preenchida pelo licitante em relação à sua proposta final, conforme anexo III deste Edital.

8.3 A Proposta de Preços deverá ser encaminhada pelo licitante exclusivamente via sistema, no prazo de 2(duas) horas, contado da solicitação do Pregoeiro, com os respectivos valores adequados ao lance vencedor e será analisada pelo Pregoeiro no momento da aceitação do lance vencedor.

8.4 A inexequibilidade dos valores referentes a itens isolados da Planilha de Custos e Formação de Preços não caracteriza motivo suficiente para a desclassificação da proposta, desde que não contrariem exigências legais.

8.5 Será desclassificada a proposta ou o lance vencedor, nos termos do item 9.1 do Anexo VII-A da In SEGES/MPDG n. 5/2017, que:

8.5.1 não estiver em conformidade com os requisitos estabelecidos neste edital;

8.5.2 contenha vício insanável ou ilegalidade;

8.5.3 não apresente as especificações técnicas exigidas pelo Termo de Referência;

8.5.4 apresentar preço final superior ao preço máximo fixado (Acórdão nº 1455/2018-TCU – Plenário), desconto menor do que o mínimo exigido, ou que apresentar preço manifestamente inexequível.

8.6 Quando o licitante não conseguir comprovar que possui ou possuirá recursos suficientes para executar a contento o objeto, será considerada inexequível a proposta de preços ou menor lance que:

8.7 for insuficiente para a cobertura dos custos da contratação, apresente preços global ou unitários simbólicos, irrisórios ou de valor zero, incompatíveis com os preços dos insumos e salários de mercado, acrescidos dos respectivos encargos, ainda que o ato convocatório da licitação não tenha estabelecido limites mínimos, exceto quando se referirem a materiais e instalações de propriedade do próprio licitante, para os quais ele renuncie a parcela ou à totalidade da remuneração.

8.8 apresentar um ou mais valores da planilha de custo que sejam inferiores àqueles fixados em instrumentos de caráter normativo obrigatório, tais como leis, medidas provisórias e convenções coletivas de trabalho vigentes.

8.9 Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, na forma do § 3° do artigo 43 da Lei n° 8.666, de 1993 e a exemplo das enumeradas no item 9.4 do Anexo VII-A da IN SEGES/MPDG N. 5, de 2017, para que a empresa comprove a exequibilidade da proposta.

8.10 Quando o licitante apresentar preço final inferior a 30% (trinta por cento) da média dos preços ofertados para o mesmo item, e a inexequibilidade da proposta não for flagrante e evidente pela análise da planilha de custos, não sendo possível a sua imediata desclassificação, será obrigatória a realização de diligências para aferir a legalidade e exequibilidade da proposta.

8.11 Qualquer interessado poderá requerer que se realizem diligências para aferir a exequibilidade e a legalidade das propostas, devendo apresentar as provas ou os indícios que fundamentam a suspeita.

8.12 Na hipótese de necessidade de suspensão de sessão pública para a realização de diligências, com vista ao saneamento das propostas, a sessão pública somente poderá ser reiniciada mediante aviso prévio no sistema com, no mínimo, vinte e quatro horas de antecedência, e a ocorrência será registrada em ata.

8.13 O Pregoeiro poderá convocar o licitante para enviar documento digital complementar, por meio de funcionalidade disponível no sistema, no prazo de duas horas, sob pena de não aceitação da proposta.

8.14 É facultado ao pregoeiro prorrogar o prazo estabelecido, a partir de solicitação fundamentada feita no chat pelo licitante, antes de findo o prazo

8.15 Dentre os documentos passíveis de solicitação pelo Pregoeiro, destacam-se as a Proposta Comercial readequadas com o valor final ofertado.

8.16 Todos os dados informados pelo licitante em sua Proposta deverão refletir com fidelidade os custos especificados e a margem de lucro pretendida.

8.17 O Pregoeiro analisará a compatibilidade dos preços unitários apresentados na Proposta Comercial com aqueles praticados no mercado em relação aos insumos e também quanto aos salários das categorias envolvidas na contratação;

8.18 **Para fins de análise da proposta quanto ao cumprimento das especificações do objeto, poderá ser colhida a manifestação escrita do setor requisitante do serviço ou da área especializada no objeto.**

8.19 Se a proposta ou lance vencedor for desclassificado, o Pregoeiro examinará a proposta ou lance subsequente, e, assim sucessivamente, na ordem de classificação.

8.20 Havendo necessidade, o Pregoeiro suspenderá a sessão, informando no "chat" a nova data e horário para a sua continuidade.

8.21 Nos itens não exclusivos para a participação de microempresas e empresas de pequeno porte, sempre que a proposta não for aceita, e antes de o Pregoeiro passar à subsequente, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos artigos 44 e 45 da LC nº 123, de 2006, seguindo-se a disciplina antes estabelecida, se for o caso. Encerrada a análise quanto à aceitação da proposta, o pregoeiro verificará a habilitação do licitante, observado o disposto neste Edital.

9 DA HABILITAÇÃO

9.1 Como condição prévia ao exame da documentação de habilitação do licitante detentor da proposta classificada em primeiro lugar, o Pregoeiro verificará o eventual descumprimento das condições de participação, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

a) SICAF;

b) Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS, mantido pela Controladoria-Geral da União (www.portaldatransparencia.gov.br/ceis);

c) Cadastro Nacional de Condenações Cíveis por Atos de Improbidade Administrativa, mantido pelo Conselho Nacional de Justiça (www.cnj.jus.br/improbidade_adm/consultar_requerido.php).

d) Lista de Inidôneos e o Cadastro Integrado de Condenações por Ilícitos Administrativos - CADICON, mantidos pelo Tribunal de Contas da União - TCU;

9.2 Para a consulta de licitantes pessoa jurídica poderá haver a substituição das consultas das alíneas "b", "c" e "d" acima pela Consulta Consolidada de Pessoa Jurídica do TCU (https://certidoesapf.apps.tcu.gov.br/)

9.3 A consulta aos cadastros será realizada em nome da empresa licitante e também de seu sócio majoritário, por força do artigo 12 da Lei n° 8.429, de 1992, que prevê, dentre as sanções impostas ao responsável pela prática de ato de improbidade administrativa, a proibição de contratar com o Poder Público, inclusive por intermédio de pessoa jurídica da qual seja sócio majoritário.

9.4 Caso conste na Consulta de Situação do Fornecedor a existência de Ocorrências Impeditivas Indiretas, o gestor diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas.

9.5 A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros.

9.6 O licitante será convocado para manifestação previamente à sua desclassificação.

9.7 Constatada a existência de sanção, o Pregoeiro reputará o licitante inabilitado, por falta de condição de participação.

9.8 No caso de inabilitação, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos arts. 44 e 45 da Lei Complementar nº 123, de 2006, seguindo-se a disciplina antes estabelecida para aceitação da proposta subsequente.

9.9 Caso atendidas as condições de participação, a habilitação do licitante será verificada por meio do SICAF, nos documentos por ele abrangidos, em relação à habilitação jurídica, à regularidade fiscal e à qualificação econômica financeira, conforme o disposto na Instrução Normativa SEGES/MP nº 03, de 2018.

9.10 O interessado, para efeitos de habilitação prevista na Instrução Normativa SEGES/MP nº 03, de 2018 mediante utilização do sistema, deverá atender às condições exigidas no cadastramento no SICAF até o terceiro dia útil anterior à data prevista para recebimento das propostas;

9.11 É dever do licitante atualizar previamente as comprovações constantes do SICAF para que estejam vigentes na data da abertura da sessão pública, ou encaminhar, em conjunto com a apresentação da proposta, a respectiva documentação atualizada.

9.12 O descumprimento do subitem acima implicará a inabilitação do licitante, exceto se a consulta aos sítios eletrônicos oficiais emissores de certidões feita pelo Pregoeiro lograr êxito em encontrar a(s) certidão(ões) válida(s), conforme art. 43, §3º, do Decreto 10.024, de 2019.

9.13 Havendo a necessidade de envio de documentos de habilitação complementares, necessários à confirmação daqueles exigidos neste Edital e já apresentados, o licitante será convocado a encaminhá-los, em formato digital, via sistema, no prazo de 02 (duas) horas [mínimo de duas horas], sob pena de inabilitação.

9.14 Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante a apresentação dos documentos originais não-digitais quando houver dúvida em relação à integridade do documento digital .

9.15 Não serão aceitos documentos de habilitação com indicação de CNPJ/CPF diferentes, salvo aqueles legalmente permitidos.

9.16 Se o licitante for a matriz, todos os documentos deverão estar em nome da matriz, e se o licitante for a filial, todos os documentos deverão estar em nome da filial, exceto aqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.

9.17 Serão aceitos registros de CNPJ de licitante matriz e filial com diferentes números de documentos pertinentes ao CND e ao CRF/FGTS, quando for comprovada a centralização do recolhimento dessas contribuições.

9.18 Ressalvado o disposto do item 5.3, os licitantes deverão encaminhar, nos termos deste Edital, a documentação nos itens a seguir, para fins de habilitação.

9.19 Habilitação jurídica:

9.19.1 *no caso de empresário individual, inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;*

9.19.2 Em se tratando de Microempreendedor Individual – MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio www.portaldoempreendedor.gov.br;

9.19.3 No caso de sociedade empresária ou empresa individual de responsabilidade limitada - EIRELI: ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado na Junta Comercial da respectiva sede, acompanhado de documento comprobatório de seus administradores;

9.19.4 inscrição no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz, no caso de ser o participante sucursal, filial ou agência;

9.19.5 No caso de sociedade simples: inscrição do ato constitutivo no Registro Civil das Pessoas Jurídicas do local de sua sede, acompanhada de prova da indicação dos seus administradores;

9.19.6 decreto de autorização, em se tratando de sociedade empresária estrangeira em funcionamento no País;

9.19.7 Os documentos acima deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

9.20 Regularidade fiscal e trabalhista:

9.20.1 prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;

9.20.2 prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02/10/2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

9.20.3 prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

9.20.4 prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943;

9.20.5 prova de inscrição no cadastro de contribuintes municipal, relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

9.20.6 prova de regularidade com a Fazenda Municipal do domicílio ou sede do licitante, relativa à atividade em cujo exercício contrata ou concorre;

9.20.7 caso o licitante seja considerado isento dos tributos municipais relacionados ao objeto licitatório, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda Municipal do seu domicílio ou sede, ou outra equivalente, na forma da lei;

9.21 Qualificação Econômico-Financeira:

9.21.1 certidão negativa de falência expedida pelo distribuidor da sede do licitante;

9.21.2 balanço patrimonial e demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, que comprovem a boa situação financeira da empresa, vedada a sua substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais quando encerrado há mais de 3 (três) meses da data de apresentação da proposta;

9.21.3 no caso de empresa constituída no exercício social vigente, admite-se a apresentação de balanço patrimonial e demonstrações contábeis referentes ao período de existência da sociedade;

9.21.4 é admissível o balanço intermediário, se decorrer de lei ou contrato/estatuto social.

9.21.5 comprovação da boa situação financeira da empresa mediante obtenção de índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), superiores a 1 (um), obtidos pela aplicação das seguintes fórmulas:

LG =	Ativo Circulante + Realizável a Longo Prazo
	Passivo Circulante + Passivo Não Circulante

SG =	Ativo Total
	Passivo Circulante + Passivo Não Circulante

LC =	Ativo Circulante
	Passivo Circulante

9.21.6 As empresas, , que apresentarem resultado inferior ou igual a 1(um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), deverão comprovar patrimônio líquido de ...(....) do valor total estimado da contratação ou do item pertinente.

9.22 Qualificação Técnica:

9.22.1 Comprovação de aptidão para a prestação dos serviços em características, quantidades e prazos compatíveis com o objeto desta licitação, ou com o item pertinente, mediante a apresentação de atestado(s) fornecido(s) por pessoas jurídicas de direito público ou privado, nas condições descritas no item 12 - critérios de habilitação técnica no Termo de Referencia(parte integrante do Edital).

9.22.2 Os atestados deverão referir-se a serviços prestados no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente;

9.22.3 Somente serão aceitos atestados expedidos após a conclusão do contrato ou se decorrido, pelo menos, um ano do início de sua execução, exceto se firmado para ser executado em prazo inferior, conforme item 10.8 do Anexo VII-A da IN SEGES/MPDG n. 5, de 2017.

9.22.4 *Poderá ser admitida, para fins de comprovação de quantitativo mínimo do serviço, a apresentação de diferentes atestados de serviços executados de forma concomitante, pois essa situação se equivale, para fins de comprovação de capacidade técnico-operacional, a uma única contratação, nos termos do item 10.9 do Anexo VII-A da IN SEGES/MPDG n. 5/2017.*

9.22.5 O licitante disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados apresentados, apresentando, dentre outros documentos, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foram prestados os serviços, consoante o disposto no item 10.10 do Anexo VII-A da IN SEGES/MPDG n. 5/2017.

9.22.6 O licitante enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado (a) da prova de inscrição nos cadastros de contribuintes estadual e municipal e (b) da apresentação do balanço patrimonial e das demonstrações contábeis do último exercício.

9.22.7 A existência de restrição relativamente à regularidade fiscal e trabalhista não impede que a licitante qualificada como microempresa ou empresa de pequeno porte seja declarada vencedora, uma vez que atenda a todas as demais exigências do edital.

9.22.8 A declaração do vencedor acontecerá no momento imediatamente posterior à fase de habilitação.

9.22.9 Caso a proposta mais vantajosa seja ofertada por microempresa, empresa de pequeno porte ou sociedade cooperativa equiparada, e uma vez constatada a existência de alguma restrição no que tange à regularidade fiscal e trabalhista, a mesma será convocada para, no prazo de 5 (cinco) dias úteis, após a declaração do vencedor, comprovar a regularização. O prazo poderá ser prorrogado por igual período, a critério da administração pública, quando requerida pelo licitante, mediante apresentação de justificativa.

9.22.10 A não-regularização fiscal e trabalhista no prazo previsto no subitem anterior acarretará a inabilitação do licitante, sem prejuízo das sanções previstas neste Edital, sendo facultada a convocação dos licitantes remanescentes, na ordem de classificação. Se, na ordem de classificação, seguir-se outra microempresa, empresa de pequeno porte ou sociedade cooperativa com alguma restrição na documentação fiscal e trabalhista, será concedido o mesmo prazo para regularização.

9.22.11 Havendo necessidade de analisar minuciosamente os documentos exigidos, o Pregoeiro suspenderá a sessão, informando no "chat" a nova data e horário para a continuidade da mesma.

9.22.12 Será inabilitado o licitante que não comprovar sua habilitação, seja por não apresentar quaisquer dos documentos exigidos, ou apresentá-los em desacordo com o estabelecido neste Edital.

9.22.13 Nos itens não exclusivos a microempresas e empresas de pequeno porte, em havendo inabilitação, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos artigos 44 e 45 da LC nº 123, de 2006, seguindo-se a disciplina antes estabelecida para aceitação da proposta subsequente.

9.22.14 Constatado o atendimento às exigências de habilitação fixadas no Edital, o licitante será declarado vencedor.

10 DO ENCAMINHAMENTO DA PROPOSTA VENCEDORA

10.1 A proposta final do licitante declarado vencedor deverá ser encaminhada no prazo de de duas horas, a contar da solicitação do Pregoeiro no sistema eletrônico e deverá:

10.1.1 ser redigida em língua portuguesa, datilografada ou digitada, em uma via, sem emendas, rasuras, entrelinhas ou ressalvas, devendo a última folha ser assinada e as demais rubricadas pelo licitante ou seu representante legal.

10.1.2 apresentar -se, devidamente ajustada ao lance vencedor, em conformidade com o modelo anexo a este instrumento convocatório.

10.1.3 conter a indicação do banco, número da conta e agência do licitante vencedor, para fins de pagamento.

10.2 A proposta final deverá ser documentada nos autos e será levada em consideração no decorrer da execução do contrato e aplicação de eventual sanção à Contratada, se for o caso.

10.3 Todas as especificações do objeto contidas na proposta vinculam a Contratada.

10.4 Os preços deverão ser expressos em moeda corrente nacional, o valor unitário em algarismos e o valor global em algarismos e por extenso (art. 5º da Lei nº 8.666/93).

10.5 Ocorrendo divergência entre os preços unitários e o preço global, prevalecerão os primeiros; no caso de divergência entre os valores numéricos e os valores expressos por extenso, prevalecerão estes últimos.

10.6 A oferta deverá ser firme e precisa, limitada, rigorosamente, ao objeto deste Edital, sem conter alternativas de preço ou de qualquer outra condição que induza o julgamento a mais de um resultado, sob pena de desclassificação.

10.7 A proposta deverá obedecer aos termos deste Edital e seus Anexos, não sendo considerada aquela que não corresponda às especificações ali contidas ou que estabeleça vínculo à proposta de outro licitante.

10.8 As propostas que contenham a descrição do objeto, o valor e os documentos complementares estarão disponíveis na internet, após a homologação.

11 DOS RECURSOS

11.1 O Pregoeiro declarará o vencedor e, depois de decorrida a fase de regularização fiscal e trabalhista de microempresa ou empresa de pequeno porte, se for o caso, concederá o prazo de no mínimo trinta minutos, para que qualquer licitante manifeste a intenção de recorrer, de forma motivada, isto é, indicando contra qual(is) decisão(ões) pretende recorrer e por quais motivos, em campo próprio do sistema.

11.2 Havendo quem se manifeste, caberá ao Pregoeiro verificar a tempestividade e a existência de motivação da intenção de recorrer, para decidir se admite ou não o recurso, fundamentadamente.

11.3 Nesse momento o Pregoeiro não adentrará no mérito recursal, mas apenas verificará as condições de admissibilidade do recurso.

11.4 A falta de manifestação motivada do licitante quanto à intenção de recorrer importará a decadência desse direito.

11.5 Uma vez admitido o recurso, o recorrente terá, a partir de então, o prazo de três dias para apresentar as razões, pelo sistema eletrônico, ficando os demais licitantes, desde logo, intimados para, querendo, apresentarem contrarrazões também pelo sistema eletrônico, em outros três dias, que começarão a contar do término do prazo do recorrente, sendo-lhes assegurada vista imediata dos elementos indispensáveis à defesa de seus interesses.

11.6 O acolhimento do recurso invalida tão somente os atos insuscetíveis de aproveitamento.

11.7 Os autos do processo permanecerão com vista franqueada aos interessados, no endereço constante neste Edital.

12 DA REABERTURA DA SESSÃO PÚBLICA

12.1 A sessão pública poderá ser reaberta:

Nas hipóteses de provimento de recurso que leve à anulação de atos anteriores à realização da sessão pública precedente ou em que seja anulada a própria sessão pública, situação em que serão repetidos os atos anulados e os que dele dependam.

Quando houver erro na aceitação do preço melhor classificado ou quando o licitante declarado vencedor não assinar o contrato, não retirar o instrumento equivalente ou não comprovar a regularização fiscal e trabalhista, nos termos

do art. 43, §1º da LC nº 123/2006, serão adotados os procedimentos imediatamente posteriores ao encerramento da etapa de lances.

12.2 Todos os licitantes remanescentes deverão ser convocados para acompanhar a sessão reaberta.

12.3 A convocação se dará por meio do sistema eletrônico ("chat"), e-mail, de acordo com a fase do procedimento licitatório.

12.4 A convocação feita por e-mail dar-se-á de acordo com os dados contidos no SICAF, sendo responsabilidade do licitante manter seus dados cadastrais atualizados.

13 DA ADJUDICAÇÃO E HOMOLOGAÇÃO

13.1 O objeto da licitação será adjudicado ao licitante declarado vencedor, por ato do Pregoeiro, caso não haja interposição de recurso, ou pela autoridade competente, após a regular decisão dos recursos apresentados.

13.2 Após a fase recursal, constatada a regularidade dos atos praticados, a autoridade competente homologará o procedimento licitatório.

14 DO TERMO DE CONTRATO OU INSTRUMENTO EQUIVALENTE

14.1 Após a homologação da licitação, em sendo realizada a contratação, será firmado Termo de Contrato ou emitido instrumento equivalente.

14.2 O adjudicatário terá o prazo de 10(dez) dias úteis, contados a partir da data de sua convocação, para assinar o Termo de Contrato ou aceitar instrumento equivalente, conforme o caso (Nota de Empenho/Carta Contrato/Autorização), sob pena de decair do direito à contratação, sem prejuízo das sanções previstas neste Edital.

14.3 Alternativamente à convocação para comparecer perante o órgão ou entidade para a assinatura do Termo de Contrato, a Administração poderá encaminhá-lo para assinatura, mediante correspondência postal com aviso de recebimento (AR) ou meio eletrônico, para que seja assinado e devolvido no prazo de10 (DEZ) dias, a contar da data de seu recebimento.

14.4 O prazo previsto no subitem anterior poderá ser prorrogado, por igual período, por solicitação justificada do adjudicatário e aceita pela Administração.

14.5 O Aceite da Nota de Empenho ou do instrumento equivalente, emitida à empresa adjudicada, implica no reconhecimento de que:

14.5.1 referida Nota está substituindo o contrato, aplicando-se à relação de negócios ali estabelecida as disposições da Lei nº 8.666, de 1993;

14.5.2 a contratada se vincula à sua proposta e às previsões contidas no edital e seus anexos;

14.5.3 a contratada reconhece que as hipóteses de rescisão são aquelas previstas nos artigos 77 e 78 da Lei nº 8.666/93 e reconhece os direitos da Administração previstos nos artigos 79 e 80 da mesma Lei.

14.6 O prazo de vigência da contratação será conforme previsão *no instrumento contratual ou no termo de referência* SUBITEM 15.8

14.7 Previamente à contratação a Administração realizará consulta ao Sicaf para identificar possível suspensão temporária de participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas, observado o disposto no art. 29, da Instrução Normativa nº 3, de 26 de abril de 2018, e nos termos do art. 6º, III, da Lei nº 10.522, de 19 de julho de 2002, consulta prévia ao CADIN.

14.8 Nos casos em que houver necessidade de assinatura do instrumento de contrato, e o fornecedor não estiver inscrito no SICAF, este deverá proceder ao seu cadastramento, sem ônus, antes da contratação.

14.9 Na hipótese de irregularidade do registro no SICAF, o contratado deverá regularizar a sua situação perante o cadastro no prazo de até 05 (cinco) dias úteis, sob pena de aplicação das penalidades previstas no edital e anexos.

14.10 Na assinatura do contrato ou da ata de registro de preços, será exigida a comprovação das condições de habilitação consignadas no edital, que deverão ser mantidas pelo licitante durante a vigência do contrato ou da ata de registro de preços.

14.11 Na hipótese de o vencedor da licitação não comprovar as condições de habilitação consignadas no edital ou se recusar a assinar o contrato ou a ata de registro de preços, a Administração, sem prejuízo da aplicação das sanções das demais cominações legais cabíveis a esse licitante, poderá convocar outro licitante, respeitada a ordem de classificação, para, após a comprovação dos requisitos para habilitação, analisada a proposta e eventuais documentos complementares e, feita a negociação, assinar o contrato ou a ata de registro de preços.

15 DO REAJUSTAMENTO EM SENTIDO GERAL

15.1 As regras acerca do reajustamento em sentido geral do valor contratual são as estabelecidas no Termo de Referência, anexo a este Edital.

16 DO RECEBIMENTO DO OBJETO E DA FISCALIZAÇÃO

16.1 Os critérios de recebimento e aceitação do objeto e de fiscalização estão previstos no Termo de Referência.

17 DAS OBRIGAÇÕES DA CONTRATANTE E DA CONTRATADA

17.1 As obrigações da Contratante e da Contratada são as estabelecidas no Termo de Referência.

18 DO PAGAMENTO

18.1 As regras acerca do pagamento são as estabelecidas no Termo de **Referência, anexo a este Edital.**

19 DAS SANÇÕES ADMINISTRATIVAS.

19.1 Comete infração administrativa, nos termos da Lei nº 10.520, de 2002, o licitante/adjudicatário que:

19.1.1 não assinar o termo de contrato ou aceitar/retirar o instrumento equivalente, quando convocado dentro do prazo de validade da proposta;

19.1.2 não assinar a ata de registro de preços, quando cabível;

19.1.3 apresentar documentação falsa;

19.1.4 deixar de entregar os documentos exigidos no certame;

19.1.5 ensejar o retardamento da execução do objeto;

19.1.6 não mantiver a proposta;

19.1.7 cometer fraude fiscal;

19.1.8 comportar-se de modo inidôneo;

19.2 As sanções do item acima também se aplicam aos integrantes do cadastro de reserva, em pregão para registro de preços que, convocados, não honrarem o compromisso assumido injustificadamente.

19.3 Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os licitantes, em qualquer momento da licitação, mesmo após o encerramento da fase de lances.

19.4 O licitante/adjudicatário que cometer qualquer das infrações discriminadas nos subitens anteriores ficará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

19.4.1 Advertência por faltas leves, assim entendidas como aquelas que não acarretarem prejuízos significativos ao objeto da contratação;

19.4.2 Multa de 5.% (.cinco por cento) sobre o valor estimado do(s) item(s) prejudicado(s) pela conduta do licitante;

19.4.3 Suspensão de licitar e impedimento de contratar com o órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente, pelo prazo de até dois anos;

19.4.4 Impedimento de licitar e de contratar com a União e descredenciamento no SICAF, pelo prazo de até cinco anos;

19.4.5 Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a Contratada ressarcir a Contratante pelos prejuízos causados;

19.5 A penalidade de multa pode ser aplicada cumulativamente com as demais sanções.

19.6 Se, durante o processo de aplicação de penalidade, se houver indícios de prática de infração administrativa tipificada pela Lei nº 12.846, de 1º de agosto de 2013, como ato lesivo à administração pública nacional ou estrangeira, cópias do processo administrativo necessárias à apuração da responsabilidade da empresa deverão ser remetidas à autoridade competente, com despacho fundamentado, para ciência e decisão sobre a eventual instauração de investigação preliminar ou Processo Administrativo de Responsabilização – PAR.

19.7 A apuração e o julgamento das demais infrações administrativas não consideradas como ato lesivo à Administração Pública nacional ou estrangeira nos termos da Lei nº 12.846, de 1º de agosto de 2013, seguirão seu rito normal na unidade administrativa.

19.8 O processamento do PAR não interfere no seguimento regular dos processos administrativos específicos para apuração da ocorrência de danos e prejuízos à Administração Pública Federal resultantes de ato lesivo cometido por pessoa jurídica, com ou sem a participação de agente público.

19.9 Caso o valor da multa não seja suficiente para cobrir os prejuízos causados pela conduta do licitante, a União ou Entidade poderá cobrar o valor remanescente judicialmente, conforme artigo 419 do Código Civil.

19.10 A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa ao licitante/adjudicatário, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente na Lei nº 9.784, de 1999.

19.11 A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

19.12 As penalidades serão obrigatoriamente registradas no SICAF.

19.13 As sanções por atos praticados no decorrer da contratação estão previstas no Termo de Referência.

20 DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

20.1 Até 03 (três) dias úteis antes da data designada para a abertura da sessão pública, qualquer pessoa poderá impugnar este Edital.

20.2 A impugnação poderá ser realizada por forma eletrônica, pelo e-mail licitação@an.gov.br.

20.3 Caberá ao Pregoeiro, auxiliado pelos responsáveis pela elaboração deste Edital e seus anexos, decidir sobre a impugnação no prazo de até dois dias úteis contados da data de recebimento da impugnação.

20.4 Acolhida a impugnação, será definida e publicada nova data para a realização do certame.

20.5 Os pedidos de esclarecimentos referentes a este processo licitatório deverão ser enviados ao Pregoeiro, até 03 (três) dias úteis anteriores à data designada para abertura da sessão pública, exclusivamente por meio eletrônico via internet, no endereço indicado no Edital.

20.6 O pregoeiro responderá aos pedidos de esclarecimentos no prazo de dois dias úteis, contados da data do recebimento do pedido e poderá requisitar subsídios formais aos responsáveis pela elaboração do edital e dos anexos

20.7 As impugnações e pedidos de esclarecimentos não suspendem os prazos previstos no certame.

20.8 A concessão de efeito suspensivo à impugnação é medida excepcional e deverá ser motivada pelo pregoeiro, nos autos do processo de licitação.

20.9 As respostas aos pedidos de esclarecimentos serão divulgadas pelo sistema e vincularão os participantes e a administração.

21 DAS DISPOSIÇÕES GERAIS

21.1 Da sessão pública do Pregão divulgar-se-á Ata no sistema eletrônico.

21.2 Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário anteriormente estabelecido, desde que não haja comunicação em contrário, pelo Pregoeiro.

21.3 Todas as referências de tempo no Edital, no aviso e durante a sessão pública observarão o horário de Brasília – DF.

21.4 No julgamento das propostas e da habilitação, o Pregoeiro poderá sanar erros ou falhas que não alterem a substância das propostas, dos documentos e sua validade jurídica, mediante despacho fundamentado, registrado em ata e acessível a todos, atribuindo-lhes validade e eficácia para fins de habilitação e classificação.

21.5 A homologação do resultado desta licitação não implicará direito à contratação.

21.6 As normas disciplinadoras da licitação serão sempre interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse da Administração, o princípio da isonomia, a finalidade e a segurança da contratação.

21.7 Os licitantes assumem todos os custos de preparação e apresentação de suas propostas e a Administração não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório.

21.8 Na contagem dos prazos estabelecidos neste Edital e seus Anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento. Só se iniciam e vencem os prazos em dias de expediente na Administração.

21.9 O desatendimento de exigências formais não essenciais não importará o afastamento do licitante, desde que seja possível o aproveitamento do ato, observados os princípios da isonomia e do interesse público.

21.10 Em caso de divergência entre disposições deste Edital e de seus anexos ou demais peças que compõem o processo, prevalecerá as deste Edital.

21.11 O Edital está disponibilizado, na íntegra, no endereço eletrônico www.comprasgovernamentais.gov.br,

21.12 Os autos do processo administrativo permanecerão com vista franqueada aos interessados.

21.13 Integram este Edital, para todos os fins e efeitos, os seguintes anexos:

ANEXO I DO EDITAL- Termo de Referência; DOC SEI N. 0062672 E SEUS ANEXOS DESCRITOS NO TR :

ANEXO I DO TR - Modelo de Termo de Recebimento Provisório (SEI nº 0005993)

ANEXO II DO TR- Modelo de Termo de Recebimento Definitivo (SEI nº 0005994)

ANEXO III DO TR- Ordem de Serviço/Recebimento de Bens (SEI nº 0005996).

ANEXO IV DO TR - Termo de Compromisso de Manutenção de Sigilo (SEI nº 0005997)

ANEXO II DO EDITAL – MInuta de Termo de Contrato

Rio de Janeiro, 19 de Novembro de 2020

COLOG/Equipe de Compras/Núcleo de Licitações

TERMO DE CONTRATO

COMPRA

TERMO DE CONTRATO DE COMPRA Nº ...../...., QUE FAZEM ENTRE SI O(A)..... E A EMPRESA .....

A União / Autarquia ..... / Fundação ....., (utilizar a menção à União somente se for órgão da Administração Direta, caso contrário incluir o nome da autarquia ou fundação conforme o caso) por intermédio do(a) ..... (órgão) contratante), com sede no(a) ....., na cidade de ..... /Estado ..., inscrito(a) no CNPJ sob o nº ....., neste ato representado(a) pelo(a) .....(*cargo e nome*), nomeado(a) pela Portaria nº ....., de ..... de ..... de 20..., publicada no *DOU* de ..... de ..... de ....., portador da matrícula funcional nº .....,., doravante denominada CONTRATANTE, e o(a) ..... inscrito(a) no CNPJ/MF sob o nº ....., sediado(a) na ....., em ..... doravante designada CONTRATADA, neste ato representada pelo(a) Sr.(a) ....., portador(a) da Carteira de Identidade nº ....., expedida pela (o) ....., e CPF nº ....., tendo em vista o que consta no Processo nº ..... e em observância às disposições da Lei nº 8.666, de 21 de junho de 1993, da Lei nº 10.520, de 17 de julho de 2002 e na Lei nº 8.078, de 1990 - Código de Defesa do Consumidor, , resolvem celebrar o presente Termo de Contrato, decorrente do Pregão nº ...../20...., mediante as cláusulas e condições a seguir enunciadas.

1. CLÁUSULA PRIMEIRA – OBJETO

1.1. O objeto do presente Termo de Contrato é a aquisição de ....., conforme especificações e quantitativos estabelecidos no Termo de Referência, anexo do Edital.

1.2. Este Termo de Contrato vincula-se ao Edital do Pregão, identificado no preâmbulo e à proposta vencedora, independentemente de transcrição.

1.3. Discriminação do objeto:

ITEM	DESCRIÇÃO/ ESPECIFICAÇÃO	IDENTIFICAÇÃO CATMAT	UNIDADE DE MEDIDA	QUANTIDADE	VALOR
1					

2. CLÁUSULA SEGUNDA – VIGÊNCIA

2.1. O prazo de vigência deste Termo de Contrato é aquele fixado no Termo de Referência, com início na data de ____/____/_____ e encerramento em ____/____/_____, prorrogável na forma do art. 57, §1º, da Lei nº 8.666, de 1993.

3. CLÁUSULA TERCEIRA – PREÇO

3.1. O valor do presente Termo de Contrato é de R$ ..... (.....).

3.2. No valor acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução contratual, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

4. CLÁUSULA QUARTA – DOTAÇÃO ORÇAMENTÁRIA

4.1. As despesas decorrentes desta contratação estão programadas em dotação orçamentária própria, prevista no orçamento da União, para o exercício de *2020*, na classificação abaixo:

Gestão/Unidade:

Fonte:

Programa de Trabalho:

Elemento de Despesa:

PI:

5. CLÁUSULA QUINTA – PAGAMENTO

5.1. O prazo para pagamento e demais condições a ele referentes encontram-se no Termo de Referência.

6. CLÁUSULA SEXTA – REAJUSTE

6.1. As regras acerca do reajuste do valor contratual são as estabelecidas no Termo de Referência, anexo a este Contrato.

7. CLÁUSULA SÉTIMA – GARANTIA

7.1. Será exigida a prestação de garantia na presente contratação, conforme regras constantes do item 5 do Termo de Referência.

8. CLÁUSULA OITAVA - ENTREGA E RECEBIMENTO DO OBJETO

8.1. As condições de entrega e recebimento do objeto são aquelas previstas no Termo de Referência, anexo ao Edital.

9. CLAÚSULA NONA - FISCALIZAÇÃO

9.1. A fiscalização da execução do objeto será efetuada por Comissão/Representante designado pela CONTRATANTE, na forma estabelecida no Termo de Referência, anexo do Edital.

10. CLÁUSULA DÉCIMA – OBRIGAÇÕES DA CONTRATANTE E DA CONTRATADA

10.1. As obrigações da CONTRATANTE e da CONTRATADA são aquelas previstas no Termo de Referência, anexo do Edital.

11. CLÁUSULA DÉCIMA PRIMEIRA – SANÇÕES ADMINISTRATIVAS

11.1. As sanções referentes à execução do contrato são aquelas previstas no Termo de Referência, anexo do Edital.

12. CLÁUSULA DÉCIMA SEGUNDA – RESCISÃO

12.1. O presente Termo de Contrato poderá ser rescindido:

12.1.1. por ato unilateral e escrito da Administração, nas situações previstas nos incisos I a XII e XVII do art. 78 da Lei nº 8.666, de 1993, e com as consequências indicadas no art. 80 da

mesma Lei, sem prejuízo da aplicação das sanções previstas no Termo de Referência, anexo ao Edital;

12.1.2. amigavelmente, nos termos do art. 79, inciso II, da Lei nº 8.666, de 1993.

12.2. Os casos de rescisão contratual serão formalmente motivados, assegurando-se à CONTRATADA o direito à prévia e ampla defesa.

12.3. A CONTRATADA reconhece os direitos da CONTRATANTE em caso de rescisão administrativa prevista no art. 77 da Lei nº 8.666, de 1993.

12.4. O termo de rescisão será precedido de Relatório indicativo dos seguintes aspectos, conforme o caso:

12.4.1. Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

12.4.2. Relação dos pagamentos já efetuados e ainda devidos;

12.4.3. Indenizações e multas.

13. CLÁUSULA DÉCIMA TERCEIRA – VEDAÇÕES E PERMISSÕES

13.1. É vedado à CONTRATADA interromper a execução dos serviços sob alegação de inadimplemento por parte da CONTRATANTE, salvo nos casos previstos em lei.

13.2. É permitido à CONTRATADA caucionar ou utilizar este Termo de Contrato para qualquer operação financeira, nos termos e de acordo com os procedimentos previstos na Instrução Normativa SEGES/ME nº 53, de 8 de Julho de 2020.

13.2.1. A cessão de crédito, a ser feita mediante celebração de termo aditivo, dependerá de comprovação da regularidade fiscal e trabalhista da cessionária, bem como da certificação de que a cessionária não se encontra impedida de licitar e contratar com o Poder Público, conforme a legislação em vigor, nos termos do Parecer JL-01, de 18 de maio de 2020.

13.2.2. A crédito a ser pago à cessionária é exatamente aquele que seria destinado à cedente (contratada) pela execução do objeto contratual, com o desconto de eventuais multas, glosas e prejuízos causados à Administração, sem prejuízo da utilização de institutos tais como os da conta vinculada e do pagamento direto previstos na IN SEGES/ME nº 5, de 2017, caso aplicáveis.

14. CLÁUSULA DÉCIMA QUARTA – ALTERAÇÕES

14.1. Eventuais alterações contratuais reger-se-ão pela disciplina do art. 65 da Lei nº 8.666, de 1993.

14.2. 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.

14.3. As supressões resultantes de acordo celebrado entre as partes contratantes poderão exceder o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

15. CLÁUSULA DÉCIMA QUINTA - DOS CASOS OMISSOS.

15.1. Os casos omissos serão decididos pela CONTRATANTE, segundo as disposições contidas na Lei nº 8.666, de 1993, na Lei nº 10.520, de 2002 e demais normas federais de licitações e contratos administrativos e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078, de 1990 - Código de Defesa do Consumidor - e normas e princípios gerais dos contratos.

16. CLÁUSULA DÉCIMA SEXTA – PUBLICAÇÃO

16.1. Incumbirá à CONTRATANTE providenciar a publicação deste instrumento, por extrato, no Diário Oficial da União, no prazo previsto na Lei nº 8.666, de 1993.

17. CLÁUSULA DÉCIMA SÉTIMA – FORO

17.1. É eleito o Foro da ..... para dirimir os litígios que decorrerem da execução deste Termo de Contrato que não possam ser compostos pela conciliação, conforme art. 55, §2º da Lei nº 8.666/93.

Para firmeza e validade do pactuado, o presente Termo de Contrato foi lavrado em duas (duas) vias de igual teor, que, depois de lido e achado em ordem, vai assinado pelos contraentes.

....., ... de..... de 20.....

_____

Responsável legal da CONTRATANTE

_____

Responsável legal da CONTRATADA

TESTEMUNHAS:

1-

2-

ANEXO III DO EDITAL – Modelo de Proposta Comercial

PREGÃO ELETRÔNICO Nº 10/2020
(Processo Administrativo n°08060.000024/2019-34

ANEXO III
MODELO DE PROPOSTA DE PREÇOS

Razão Social:_____

Endereço completo: _____

Cidade:_____ UF:____ CEP.:_____ CNPJ/MF:_____

Banco: _____ Agência: _____ Conta corrente:_____

Representante Legal: _____

Identidade/Órgão Expedidor:_____ CPF/MF:_____

A Licitante acima identificada, por intermédio de seu representante legal, infra-assinado, para fins do pregão eletrônico, vem apresentar a sua proposta de preço a aquisição do (s) item (ns) abaixo, de acordo com as especificações, quantidades e as condições de fornecimento definidas no Edital do Pregão Eletrônico nº 10/2020, para atender às necessidades do Arquivo Nacional

Item	Descrição	Unid.	Qtd	Valor Unitário	Valor Total

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA
ARQUIVO NACIONAL

TERMO DE REFERÊNCIA

Processo Administrativo nº 0008227.000024/2019-34

1. DEFINIÇÃO DO OBJETO DA CONTRATAÇÃO

1.1. Aquisição de Solução de **Antivírus, Antispam,** para todo ambiente de rede do Arquivo Nacional – Ministério da Justiça e Segurança Pública, nas condições, quantidades e exigências estabelecidas neste Instrumento:

Grupo	Item	Descrição	Prazo	Quantidade
I	1	Solução corporativa de Antivírus para estações de trabalho com gerência em nuvem	36 meses	650
	2	Solução corporativa de Antivírus para Servidores Físicos e Virtuais com gerência em nuvem.	36 meses	40
	3	Solução de segurança anti-spam e e-mail gateway	12 meses	750

2. JUSTIFICATIVA E OBJETIVO DA CONTRATAÇÃO

2.1. JUSTIFICATIVA

2.1.1. A pretendida contratação faz-se indispensável, pois visa prover segurança, proteção e automação do monitoramento da rede do Arquivo Nacional e de suas respectivas unidades, de forma a minimizar e, em grande parte, coibir a contaminação dos serviços e sistemas informatizados por programas ou atividades digitais maliciosas, contribuindo para a garantia do nível mínimo adequado e desejado de proteção dos dados e informações do Órgão.

2.1.2. É fundamental manter recursos tecnológicos que garantam a segurança dos dados e informações de propriedade ou sob custódia das áreas de negócio do Arquivo Nacional, haja vista a necessidade precípua de proteção de tais ativos, de grande valor para o AN, contra os mais diversos tipos de ameaças, conforme estabelecido nas diretrizes da Política de Segurança da Informação e Comunicações – POSIC do AN.

2.1.3. A presente contratação possui duas linhas de atuação: mitigar o risco de infecção das estações trabalho e servidores por malwares, e evitar a infestação do

serviço de e-mail por mensagens do tipo Spam (Sending and Posting Advertisement in Mass).

2.1.4. Com relação ao levantamento da necessidade para cada item do objeto, cumpre informar que foram estimados de acordo com a quantidade de equipamentos, usuários e e-mails disponíveis hoje no AN, acrescido de um percentual que a Administração entende ser suficiente para atender às demandas que poderão surgir.

2.2. MOTIVAÇÃO

2.2.1. A aquisição da solução de antivírus centralizada permitirá que área responsável pela Infraestrutura de Tecnologia da Informação do Arquivo Nacional - Coordenação de Tecnologia da Informação (COTIN) mantenha os níveis exigidos de segurança das informações trafegadas em rede e os controles e políticas necessárias para certificar que tais informações estão sendo acessadas e manipuladas somente por pessoas autorizadas. Tal fato resulta em otimização da infraestrutura de segurança dos dados armazenados na instituição e, também, provê serviços com confidencialidade para as informações trafegadas e armazenadas nas estações de trabalho e nos mais diversos sistemas corpora vos do AN e suas unidades.

2.2.2. Já a aquisição da solução de antispam, também conhecida como gateway de e-mail ou gateway anti spam, tem como finalidade prevenir, detectar e remover códigos, programas ou arquivos maliciosos distribuídos por e-mail, evitando a disseminação dessas ameaças para o ambiente de rede interna, como estações de trabalho, dispositivos móveis e servidores de rede. Com o passar do tempo, esses filtros têm ficado cada vez mais eficientes, , proporcionando inteligência de detecção imediata entre um email válido e um email indesejado (fake). Os e-mails válidos são enviados para a caixa de entrada e os indesejados são marcados como Spam e armazenados em quarentenas para posterior auditoria e eventuais dúvida quanto a falso-positivo. Algumas vezes, os provedores nem mesmo enviam para sua pasta de Spam esses e-mails, bloqueando-os diretamente no sistema (antispam) do provedor.

2.2.3. Essa solução é mais uma camada de segurança utilizada para detectar e remover as mais variadas formas de ameaças virtuais, tanto para ambientes domésticos quanto para, sobretudo, redes corporativas. Em um mundo caótico onde a sofisticação dos ataques cibernéticos estão em evidência, é fundamental a adoção de modernas soluções de antispam e antivírus com capacidade de proteger contra ameaças dos tipos “objetos maliciosos Browser Helper (BHOs), sequestradores de navegador, ransomware, keyloggers, backdoors, rootkits, cavalos de tróia, worms, PEL maliciosos, dialers, fraudtools, adware e spyware, dentre outros. Além disso, picamente incluem ainda proteção contra URLs maliciosas infectadas, fraude e ataques de phishing, roubo de iden dade digital, ataques bancários on-line, técnicas de engenharia social, ameaças persistentes avançadas (APT), botnets e ataques DDoS, sendo capazes de atuar sobre as inúmeras variantes de sistemas operacionais disponíveis no mercado. O foco da solução é evitar a disseminação dessas ameaças no serviço de e-mail corporativo.

2.3. BENEFÍCIOS DIRETOS E INDIRETOS QUE RESULTARÃO DA CONTRATAÇÃO

a) Assegurar o provimento de Infraestrutura de TI segura e adequada para que as áreas finalísticas do negócio do CONTRATANTE continuem operacionais;

b) Contribuir para garantia de um nível adequado de disponibilidade, autenticidade e confiabilidade das informações produzidas e armazenadas em meios tecnológicos;

c) Oferecer maior agilidade e eficácia no tratamento de incidentes envolvendo endpoints (estações de trabalho e notebooks) comprometidos;

d) Evitar, mitigar e conter a propagação de pragas digitais facilitando o tratamento destes incidentes (vírus/malwares/spywares, spam, dentre outros) com a administração centralizada da solução de proteção;

e) Permitir o controle de acesso à rede por dispositivos computacionais, permitindo gerenciamento destes dispositivos;

f) Gerar economicidade e melhoria de qualidade do serviço de proteção de endpoints;

g) Mitigar riscos de infecção na transição entre soluções de antivírus.

2.4. JUSTIFICATIVA PARA O AGRUPAMENTO DE ITENS EM GRUPOS

2.4.1. As ferramentas de proteção de endpoint deverão ser do mesmo fabricante e fornecidas em conjunto para que sua implementação seja realizada de modo transparente para o usuário da rede de dados do Arquivo Nacional, não causando indisponibilidade de serviços e ser realizada de uma única vez.

2.4.2. Visando preservar harmonia entre todos os elementos da solução, a total interoperabilidade de componentes e a facilidade de uso e operação, os itens 1 e 2, formam um único grupo pois deverá ser de um único fabricante para que seus componentes, módulos e ou programas sejam totalmente integrados e disponibilizados em uma única console de gerência.

2.5. DA APLICAÇÃO DOS DIREITOS DE PREFERÊNCIA

2.5.1. Será assegurada, como critério de desempate, preferência de contratação para as microempresas e empresas de pequeno porte, de acordo com o art. 44 da Lei Complementar nº 123/2006.

2.5.2. Para o exercício do direito de preferência, as licitantes deverão apresentar, juntamente com a sua proposta, declaração, sob as penas da lei, de que atendem aos requisitos legais para a qualificação como microempresa ou empresa de pequeno porte, se for o caso.

2.5.3. Entende-se por empate aquelas situações em que as propostas apresentadas pelas microempresas e empresas de pequeno porte sejam iguais ou até 5% (cinco por cento) superiores à proposta mais bem classificada, desde que esta não tenha sido apresentada, também, por uma microempresa ou uma empresa de pequeno porte (art. 44, §§ 1º e 2º, e art. 45, § 2º, da Lei Complementar nº 123/2006).

2.5.4. Ocorrendo o empate, na forma do subitem anterior, será procedido da seguinte forma (art. 45 da Lei Complementar nº 123/2006):

2.5.4.1. A microempresa ou empresa de pequeno porte mais bem classificada poderá apresentar proposta de preço inferior àquela considerada vencedora do certame, no prazo máximo de 5 (cinco) minutos após o encerramento dos lances, situação em que será adjudicado em seu favor o objeto licitado (art. 45, inciso I e § 3º, da Lei Complementar nº 123/2006);

2.5.4.2. Não ocorrendo a contratação da microempresa ou empresa de pequeno porte, na forma da alínea anterior, serão convocadas as remanescentes que porventura se enquadrem na situação descrita, na ordem classificatória, para exercício do mesmo direito (art. 45, inciso II, da Lei Complementar nº 123/2006);

2.5.4.3. No caso de equivalência dos preços apresentados pelas microempresas e empresas de pequeno porte que se encontrem no intervalo de 5% (cinco por cento), será realizado, automaticamente, sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta (art. 45, inciso III, da Lei Complementar nº 123/2006);

2.5.4.4. Na hipótese da não-contratação nos termos previstos no subitem anterior, o objeto licitado será adjudicado em favor da proposta originalmente vencedora do certame (art. 45, § 1º, da Lei Complementar nº 123/2006).

2.6. CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

REGIME DE EXECUÇÃO ( ) Empreitada (**x**) Preço Global ( ) Preço Unitário
ADJUDICAÇÃO DO OBJETO ( ) Glogal (**x**) Por lote ( ) Por Item

2.7. CRITÉRIOS DE JULGAMENTO DAS PROPOSTAS

2.7.1. O julgamento das propostas de preços dar-se-á pelo critério de MENOR PREÇO, sendo declarada vencedora a empresa que apresentar o MENOR PREÇO e que atender a todos os requisitos e exigências do certame.

2.8. CRITÉRIOS AMBIENTAIS ADOTADOS (SUSTENTABILIDADE)

2.8.1. Deve-se seguir a diretriz de sustentabilidade ambiental, estabelecida na IN. 01/2010 SLTI/MPOG, qual seja: o equipamento não deve conter substâncias perigosas em concentração acima da recomendada na diretiva RoHS (Restriction of Certain Hazardous Substances), tais como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr(VI)), cádmio (Cd), bifenil-polibromados (PBBs), éteres difenilpolibromados (PBDEs).

3. DESCRIÇÃO DA SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO REQUISITOS

3.1. CARACTERÍSTICAS GERAIS DAS SOLUÇÕES DE ANTIVÍRUS PARA ESTAÇÕES E SERVIDORES.

3.1.1. Todos os componentes que fazem parte da solução, de segurança para servidores, estações de trabalho deverão ser fornecidas por um único fabricante. Não serão aceitas composições de produtos de fabricantes diferentes;

3.1.2. A console de monitoração e configuração deverá ser feita através de uma central única, baseada em web e em nuvem, que deverá conter todas a ferramentas para a monitoração e controle da proteção dos dispositivos;

3.1.3. O fabricante da console baseada em nuvem deve garantir disponibilidade de 99,8% no mês para cada funcionalidade.

3.1.4. A console de gerência em nuvem deve permitir configurar autenticação em múltiplos fatores.

3.1.5. Permitir a configuração de perfis com permissões agrupadas que possam ser vinculados às contas de acesso à solução, para possibilitar a segregação de funções.

3.1.6. A console deverá apresentar Dashboard com o resumo dos status de proteção dos computadores e usuários, bem como indicar os alertas de eventos de criticidades alta, média e informacional;

3.1.7. Permitir ao administrador criar diferentes políticas de segurança e aplicá-las a diferentes grupos de máquinas de acordo com seus atributos.

3.1.8. Deve possuir mecanismo de comunicação via API, para integração com outras soluções de segurança, como por exemplo SIEM;

3.1.9. A console deve permitir a divisão dos computadores, dentro da estrutura de gerenciamento em grupos;

3.1.10. Deve permitir sincronização com o Active Directory (AD) para gestão de usuários e grupos integrados às políticas de proteção.

3.1.11. Deve possuir a possibilidade de aplicar regras diferenciadas baseado em grupos, usuários ou dispositivos;

3.1.12. A instalação deve ser feita via cliente específico por download da gerência central e via e-mail de configuração. O instalador deverá permitir a distribuição do cliente via Active Directory (AD) para múltiplas máquina.

3.1.13. Deve ser possível a instalação dos agentes de forma manual ou remota, com suporte à distribuição do agente por ferramentas de terceiros, incluindo o System Center Configuration Manager (SCCM) da Microsoft.

3.1.14. Deve ser possível configurar parâmetros de linha de comando para configurar pelo menos os seguintes itens:

a) instalação silenciosa

b) Proxy de rede

c) Nome do dispositivo

3.1.15. O agente deve ser classificado pelo Windows como solução de Antivírus (anti-malware)

3.1.16. Deve ser possível armazenar os dados da instalação e transformar estes dados em um cache da instalação, de forma que possibilite a instalação em outros dispositivos utilizando-se deste cache com o intuito de reduzir o uso da largura de banda.

3.1.17. Deve a console ser capaz de criar e editar diferentes políticas para a aplicação das proteções exigidas e aplicadas a nível de usuários, não importando em que equipamentos eles estejam acessando;

3.1.18. Fornecer atualizações do produto e das definições de vírus e proteção contra intrusos;

3.1.19. Deve permitir exclusões de escaneamento para um determinado website, arquivo, processos ou aplicação, tanto a nível geral quanto específico em uma determinada política.

3.1.20. A console de gerenciamento deve permitir a definição de grupos de usuários com diferentes níveis de acesso as configurações, políticas e logs;

3.1.21. Atualização incremental, remota e em tempo-real, da vacina dos Antivírus e do mecanismo de verificação (Engine) dos clientes;

3.1.22. Permitir o agendamento da varredura contra vírus com a possibilidade de selecionar uma máquina, grupo de máquinas ou domínio, com periodicidade definida pelo administrador;

3.1.23. Atualização automática das assinaturas de ameaças (malwares) e políticas de prevenção desenvolvidas pelo fabricante em tempo real ou com periodicidade definida pelo administrador;

3.1.24. Utilizar protocolos seguros padrão HTTPS para comunicação entre console de gerenciamento e clientes gerenciados.

3.1.25. As mensagens geradas pelo agente deverão estar no idioma em Português ou permitir a sua edição.

3.1.26. Permitir a exportação dos relatórios gerenciais para os formatos CSV e PDF;

3.1.27. Recursos do relatório e monitoramento deverão ser nativos da própria console central de gerenciamento;

3.1.28. Possibilidade de exibir informações como nome da máquina, versão do antivírus, sistema operacional, versão da engine, data da vacina, data da última verificação, eventos recentes e status;

3.1.29. Permitir a configuração de alertas em tempo real de ameaças com envio de e-mail a usuários pré-definidos

3.1.30. Capacidade de geração de relatórios, estatísticos ou gráficos, tais como:

a) Detalhar quais usuários estão ativos, inativos ou desprotegidos, bem como detalhes dos mesmos;

b) Detalhamento dos computadores que estão ativos, inativos ou desprotegidos, bem como detalhes das varreduras e dos alertas nos computadores;

c) Detalhamento dos periféricos permitidos ou bloqueados, bem como detalhes de onde e quando cada periférico foi usado;

d) Detalhamento das principais aplicações bloqueadas e os servidores/usuários que tentaram acessá-las;.

e) Detalhamento das aplicações permitidas que foram acessadas com maior frequência e os servidores/usuários que as acessam;

f) Detalhamento dos servidores/usuários que tentaram acessar aplicações bloqueadas com maior frequência e as aplicações que eles tentaram acessar;

g) Detalhamento de todas as atividades disparadas por regras de prevenção de perda de dados.

3.1.31. A console de gerenciamento deve evidenciar de forma gráfica toda a rastreabilidade de um ataque, contendo toda a sequência de eventos que ocorreram durante a execução do malware, sendo possível ainda expandir os detalhes de cada informação e identificar informações como a causa raíz de um determinado ataque/infecção.

3.1.32. Devem ser coletadas as atividades de todos artefatos analisados, contendo informações sobre interação com outros processos, arquivos e chaves de registro acessadas/modificadas, conexões de rede realizadas, dentre outras. Deve ser possível exportar essas informações

3.1.33. Permitir isolar a máquina, de maneira que ela perca a comunicação com a

rede ou se comunique apenas com os servidores da solução ou com servidores e serviços definidos na política de isolamento.

3.1.34. O agente deve ter a capacidade de fazer o isolamento da máquina por si só, sem precisar de nenhuma integração com outros softwares ou dispositivos de rede para isso.

3.1.35. Deve ser possível ao administrador efetuar a liberação da máquina do isolamento via console de gerência ou fornecer uma chave para realizar a liberação.

3.1.36. Deverá possuir um elemento de comunicação para mensagens e notificações entre estações e a console de gerenciamento utilizando comunicação criptografada;

3.1.37. Deve fornecer solução de gerenciamento de arquivos armazenados em nuvem, garantindo que um arquivo que foi feito um upload (exemplo Dropbox), tenha o processo monitorado e gerenciado, bem como realizar automaticamente o escaneamento do arquivo contra malwares, procuradas palavras chaves ou informações confidenciais;

3.1.38. A atualização da versão deverá ser transparente para os usuários finais.

3.1.39. O agente antivírus deverá proteger laptops, desktops e servidores em tempo real, sob demanda ou agendado para detectar, bloquear e limpar todos os vírus, trojans, worms e spyware. No Windows o agente também deverá detectar PUA, adware, comportamento suspeito, controle de aplicações e dados sensíveis. O agente ainda deve fornecer controle de dispositivos terceiros e, controle de acesso a web;

3.1.40. Deve possuir mecanismo contra a desinstalação do endpoint pelo usuário e cada dispositivo deverá ter uma senha única, não sendo autorizadas soluções com uma mesma senha válida para todos os dispositivos;

3.1.41. Deve prover no endpoint a solução de HIPS (Host Intrusion Prevention System) para a detecção automática e proteção contra comportamentos maliciosos (análise de comportamento) e deverá ser atualizado automaticamente;

3.1.42. Deve prover proteção automática contra web sites infectados e maliciosos, assim como prevenir o ataque de vulnerabilidades de browser via web exploits;

3.1.43. Deve permitir a monitoração e o controle de dispositivos removíveis nos equipamentos dos usuários, como dispositivos USB, periféricos da própria estação de trabalho e redes sem fio, estando sempre atrelado ao usuário o controle e não ao dispositivo;

3.1.44. O controle de dispositivos deve ser ao nível de permissão, como somente leitura ou bloqueio;

3.1.45. Os seguintes dispositivos deverão ser, no mínimo, gerenciados: HD (hard disks) externos, pendrives USB, storages removíveis seguras, CD, DVD, Blu-ray, floppy drives, interfaces de rede sem fio, modems, bluetooth, infra-vermelho, MTP (Media Transfer Protocol) tais como Blackberry, iPhone e Android smartphone e PTP (Picture Transfer Protocol) como câmeras digitais;

3.1.46. Deve possuir funcionalidades de monitoramento do firewall local do Windows

3.1.47. A ferramenta de administração centralizada deverá gerenciar todos os componentes da proteção para estações de trabalho e servidores e deverá ser projetada para a fácil administração, supervisão e elaboração de relatórios dos endpoint e servidores;

.

3.1.48. Deverá possuir interface gráfica web, com suporte aos seguintes idiomas:

a) Inglês (padrão);

b) Português do Brasil;

3.1.49. A Console de administração deve incluir um painel com um resumo visual em tempo real para verificação do status de segurança;

3.1.50. Deverá fornecer filtros pré-construídos que permitam visualizar e corrigir apenas os computadores que precisam de atenção;

3.1.51. Deverá exibir os PCs gerenciados de acordo com critérios da categoria (detalhes do estado do computador, detalhes sobre a atualização, detalhes de avisos e erros, detalhes do antivírus, etc), e classificar os PCs em conformidade;

3.1.52. Uma vez que um problema seja identificado, deverá permitir corrigir os problemas remotamente, com no mínimo as opções abaixo:

3.1.53. Proteger o dispositivo com a opção de início de uma varredura;

3.1.54. Forçar uma atualização naquele momento;

3.1.55. Ver os detalhes dos eventos ocorridos;

3.1.56. Executar verificação completa do sistema;

3.1.57. Forçar o cumprimento de uma nova política de segurança;

3.1.58. Mover o computador para outro grupo;

3.1.59. Apagar o computador da lista;

3.1.60. Atualizar a políticas de segurança quando um computador for movido de um grupo para outro manualmente ou automaticamente;

3.1.61. Gravar um log de auditoria seguro, que monitore a atividade na console de gerenciamento para o cumprimento de regulamentações, auditorias de segurança, análise e solução de problemas forenses;

3.1.62. Deverá permitir exportar o relatório de logs de auditoria nos formatos CSV e PDF;

3.1.63. Todos os logs devem ser armazenados pelo fabricante gratuitamente por pelo menos 90 dias.

3.1.64. O agente deve ter a possibilidade de gerar um arquivo único contendo todos os logs e informações necessárias para que o suporte do fabricante possa realizar um troubleshooting avançado em casos de problemas.

3.1.65. Deve conter vários relatórios para análise e controle dos usuários e endpoints. Os relatórios deverão ser divididos, no mínimo, em relatórios de: eventos, usuários, controle de aplicativos, periféricos e web, indicando todas as funções solicitadas para os endpoints;

3.1.66. Fornecer relatórios utilizando listas ou gráficos, utilizando informações presentes na console, com no mínimo os seguintes tipos:

a) Nome do dispositivo;

b) Início da proteção;

c) Último usuário logado no dispositivo;

d) Status do escaneamento em tempo real;

e) Último update;

f) Último escaneamento realizado;

g) Status de proteção do dispositivo;

h) Grupo a qual o dispositivo faz parte;

i) Permitir a execução manual de todos estes relatórios, assim como o agendamento e envio automático por e-mail nos formatos CSV e PDF;

3.2. SOLUÇÃO DE ENDPOINT DETECTION AND RESPONSE (EDR)

3.2.1. A solução deve ter capacidade de implementar técnicas de EDR (Endpoint Detection and Response), possibilitando detecção e investigação nos endpoints com atividades suspeitas;

3.2.2. Deve ter a capacidade de submeter arquivos identificados em incidentes a uma segunda consulta a nuvem de inteligência do fabricante.

3.2.3. Em caso de incidente a solução deve mostrar a trilha da infecção de forma visual, mostrando o inicio, todas as interações do malware e o ponto final de bloqueio.

3.2.4. Após a análise da nuvem de inteligência do fabricante a solução deve apresentar um relatório sobre a ameaça contendo no mínimo:

3.2.5. Detalhes do Processo, como nome, hash, hora e data da detecção e remediação;

3.2.6. Reputação do arquivo e correlação da detecção do arquivo em outras soluções de antivírus através de bases de conhecimento como o Vírus Total;

3.2.7. Resultado da análise do arquivo suspeito pela funcionalidade de Machinne Learning;

3.2.8. Propriedades gerais do arquivo, como nome, versão, tamanho, idioma, informações de certificado;

3.2.9. A solução de EDR deverá ser integrado ao agente de antivírus a ser instalado com um com agente único, em estação de trabalho, servidores físicos e virtuais a fim de diminuir o impacto ao usuário final;

3.2.10. O gerenciamento da solução de EDR deverá ser feito a partir da mesma console de gerenciamento da solução antivírus;

3.2.11. Deve fornecer guias de repostas a incidentes, fornecendo visibilidade sobre o escopo de um ataque, como ele começou, o que foi impactado, e como responder;

3.2.12. Deve ser capaz de responder ao incidente com opção de isolamento da máquina, bloqueio e limpeza da ameaça;

3.2.13. Deve ser capaz realizar buscas de ameaças em todo o ambiente, sendo capaz de buscar por hash, nome, endereços IP, domínio ou linha de comando;

3.3. CARACTERÍSTICAS GERAIS DA SOLUÇÃO DE PROTEÇÃO PARA ESTAÇÕES DE TRABALHO

3.3.1. **Características básicas do agente de proteção contra malwares:**

3.3.1.1. Pré-execução para verificar e detectar malwares desconhecidos,

incluindo zero-days;

3.3.1.2. O agente deve buscar algum sinal de malware ativo e detectar malwares desconhecidos.

3.3.1.3. Deverá conter técnicas avançadas de detecção de malwares desconhecidos, utilizando algoritmos de inteligência artificial, como machine learning ou deep learning;

3.3.1.4. Efetuar a análise baseada em técnicas de machine learning, inteligência artificial, anti-exploits ou threat intelligence, permitindo a proteção contra-ataques que explorem vulnerabilidades, mesmo que ainda não existam patches de correção.

3.3.1.5. O agente deve ter a capacidade de submeter o arquivo desconhecido à nuvem de inteligência do fabricante para detectar a presença de ameaças;

3.3.1.6. O agente deve realizar a atualização várias vezes por dia para manter a detecção atualizada contra as ameaças mais recentes;

3.3.1.7. A solução deve manter conexão direta com banco de dados de ameaças do fabricante para uso da rede de inteligência;

3.3.1.8. Deve realizar a verificação de todos os arquivos acessados em tempo real;

3.3.1.9. Deve realizar a verificação de todos os arquivos no disco rígido em intervalos programados;

3.3.1.10. Deve realizar a limpeza do sistema automaticamente, removendo itens maliciosos detectados e aplicações potencialmente indesejáveis (PUA);

3.3.1.11. Deve proteger os navegadores Internet Explorer, Firefox, Chrome, Opera e Safari, bloqueando o acesso a sites infectados conhecidos e pela verificação dos dados baixados antes de serem executados;

3.3.1.12. Deve permitir a autorização de detecções maliciosas e excluir da varredura diretórios e arquivos específicos;

3.3.1.13. É requerida a proteção integrada, ou seja, em um único agente, contra ameaças de segurança, incluindo vírus, spyware, trojans, worms, adware e aplicativos potencialmente indesejados (PUAs);

3.3.1.14. Suportar máquinas com arquitetura 32-bit e 64-bit;

3.3.1.15. O cliente para instalação em estações de trabalho deverá ser compatível com os sistemas operacionais, Mac OS X 10.10, 10.11, 10.12, Microsoft Windows Vista, 7, 8, 8.1, 10;

3.3.1.16. O cliente para instalação em estações de trabalho deverá ser compatível com os sistemas operacionais Linux CentOS 6/7/8, Ubuntu 16/18, Debian 9/10;

3.3.1.17. Possuir a funcionalidade de proteção contra a alteração das configurações do agente, impedindo aos usuários, incluindo o administrador local, reconfigurar, desativar ou desinstalar componentes da solução de proteção;

3.3.1.18. Permitir a utilização de senha de proteção para possibilitar a reconfiguração local no cliente ou desinstalação dos componentes de proteção;

3.3.2. **Funcionalidade de Detecção e Proteção de Intrusão com as funcionalidades:**

3.3.2.1. Possuir proteção contra exploração de buffer overflow;

3.3.2.2. Possuir proteção contra ataques de Negação de Serviço;

3.3.2.3. Deverá possui atualização periódica de novas assinaturas de ataque;

3.3.2.4. Capacidade de reconhecer e bloquear automaticamente as aplicações em clientes baseando-se na impressão digital (hash) do arquivo.

3.3.2.5. Capacidade de bloqueio de ataques baseado na exploração de vulnerabilidade conhecidas;

3.3.2.6. Possuir um sistema de prevenção de intrusão no host (HIPS), que monitore o código e blocos de código que podem se comportar de forma maliciosa antes de serem executados.

3.3.2.7. Ser capaz de aplicar uma análise adicional, inspecionando finalmente o comportamento de códigos durante a execução, para detectar comportamento suspeito de aplicações, tais como buffer overflow.

3.3.2.8. Deve possuir técnicas de proteção, que inclui:

a) Análise dinâmica de código - técnica para detectar malware criptografado mais complexo;

b) Algoritmo correspondente padrão - onde os dados de entrada são comparados com um conjunto de sequências conhecidas de código já identificados como um vírus;

c) Emulação - uma técnica para a detecção de vírus polimórficos, ou seja, vírus que se escondem criptografando-se de maneira diferente cada vez que se espalham;

3.3.2.9. Detectar scripts malwares do tipo fileless que possuem seu código ofuscado, inspecionando o código de malwares quando executados diretamente em memória, utilizando os engines de AntiMalware scanning interface (AMSI) ou Early Launch antimalware (ELAM) – EAP

3.3.2.10. Proteção contra malwares que executam payloads que abrem acesso remoto a invasores, ataques conhecidos como shellcode

3.3.2.11. Proteção contra sequestro de processos do Windows, utilizando a falha do Windows CTF, publicada no CVE-2019-1162 .

3.3.2.12. Prevenir tráfego de rede mal-intencionado com inspeção de pacotes de rede

3.3.2.13. Proteção contra ataques direcionados ao sistema de criptografia do sistema de arquivos (EFS)

3.3.2.14. Bloquear ataques que tentam se passar por processos legítimos do Windows (hollowing);

3.3.2.15. Prevenir a invocação maliciosa de malwares através do Rundll

3.3.2.16. Detectar e bloquear ameaças que utilizem técnicas de ofuscação e sequestro de DLL

3.3.2.17. Detectar e bloquear técnicas de evasão, incluindo process injection e uso de executáveis legítimos do Windows para rodar scripts e ações maliciosas.

3.3.2.18. Tecnologia de redução de ameaças - detecção de prováveis ameaças por uma variedade de critérios, como extensões duplas (por exemplo. jpg.txt) ou a extensão não coincida com o tipo de arquivo verdadeiro (por exemplo, um arquivo executável ou arquivo .exe com a extensão .txt);

3.3.2.19. Verificação de ameaças web avançadas: bloqueia ameaças verificando o conteúdo em tempo real e remontando com emulação de JavaScript e análise

comportamental para identificar e parar o código malicioso de malware avançados;

3.3.3. **Funcionalidade de Antivírus e AntiSpyware:**

3.3.3.1. Proteção em tempo real contra vírus, trojans, worms, rootkits, botnets, spyware, adwares e outros tipos de códigos maliciosos.

3.3.3.2. Proteção anti-malware deverá ser nativa da solução ou incorporada automaticamente por meio de plug-ins sem a utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo fabricante.

3.3.3.3. As configurações do anti-spyware deverão ser realizadas através da mesma console do antivírus;

3.3.3.4. Permitir a configuração de ações diferenciadas para programas potencialmente indesejados ou malware, com possibilidade de inclusão de arquivos em listas de exclusão (whitelists) para que não sejam verificados pelo produto;

3.3.3.5. Permitir a varredura das ameaças da maneira manual, agendada e em tempo real na máquina do usuário;

3.3.3.6. Capacidade de detecção e reparo em tempo real de vírus de macro conhecidos e novos através do antivírus;

3.3.3.7. Capacidade de remoção automática total dos danos causados por spyware, adwares e worms, como limpeza do registro e pontos de carregamento, com opção de finalizar o processo e terminar o serviço da ameaça no momento de detecção;

3.3.3.8. A remoção automática dos danos causados deverá ser nativa do próprio antivírus; ou adicionada por plugin, desde que desenvolvido ou distribuído pelo fabricante;

3.3.3.9. Capacidade de bloquear origem de infecção através de compartilhamento de rede com opção de bloqueio da comunicação via rede;

3.3.3.10. Permitir o bloqueio da verificação de vírus em recursos mapeados da rede;

3.3.3.11. Antivírus de Web (verificação de sites e downloads contra vírus);

3.3.3.12. Controle de acesso a sites por categoria.

3.3.3.13. Proteger a navegação na web, mesmo aos usuários fora da rede, para todos os principais navegadores (IE, Firefox, Safari, Opera e Chrome), fornecendo controle da Internet independentemente do browser utilizado, como parte da solução de proteção a estações de trabalho, incluindo a análise do conteúdo baixado pelo navegador web, de forma independente do navegador usado, ou seja, sem utilizar um plugin, onde não é possível ser ignorada pelos usuários, protegendo os usuários de websites infectados e categorias específicas de websites.

3.3.3.14. O Controle da Web deve controlar o acesso a sites impróprios, com no mínimo 14 categorias de sites inadequados. Deve ainda permitir a criação de lista branca de sites sempre permitidos e lista negra de sites que devem ser bloqueados sempre;

3.3.3.15. Todas as atividades de navegação na Internet bloqueadas deverão ser enviadas para a console de gerenciamento, informando detalhes do evento e a razão para o bloqueio;

3.3.3.16. Capacidade de verificar somente arquivos novos e alterados;

3.3.3.17. Funcionalidades específicas para prevenção contra a ação de

ransomwares, tais como a capacidade de impedir a criptografia quando feita por aplicativos desconhecidos ou a capacidade de fazer backup de arquivos antes de serem criptografados para posteriormente permitir sua restauração.

3.3.4. **Funcionalidade de detecção Pró-Ativa de reconhecimento de novas ameaças:**

3.3.4.1. Funcionalidade de detecção de ameaças desconhecidas que estão em memória;

3.3.4.2. Capacidade de detecção, e bloqueio proativo de keyloggers e outros malwares não conhecidos (ataques de dia zero) através da análise de comportamento de processos em memória (heurística);

3.3.4.3. Capacidade de detecção e bloqueio de Trojans e Worms, entre outros malwares, por comportamento dos processos em memória;

3.3.4.4. Capacidade de analisar o comportamento de novos processos ao serem executados, em complemento à varredura agendada.

3.3.5. **Funcionalidade de proteção contra ransomwares:**

3.3.5.1. Para estações de trabalho, dispor de capacidade de proteção contra ransomware não baseada exclusivamente na detecção por assinaturas;

3.3.5.2. Para estações de trabalho, dispor de capacidade de remediação da ação de criptografia maliciosa dos ransomwares;

3.3.5.3. Para servidores, dispor de capacidade de prevenção contra a ação de criptografia maliciosa executada por ransomwares, possibilitando ainda o bloqueio dos computadores de onde partirem tal ação;

3.3.6. **Funcionalidade de Controle de aplicações e dispositivos:**

3.3.6.1. Possuir controle de aplicativos para monitorar e impedir que os usuários executem ou instalem aplicações que podem afetar a produtividade ou o desempenho da rede;

3.3.6.2. Atualiza automaticamente a lista de aplicativos que podem ser controlados, permitindo que aplicativos específicos ou categorias específicas de aplicações possa ser liberada ou bloqueada;

3.3.6.3. Verificar a identidade de um aplicativo de maneira genérica para detectar todas as suas versões. Permitir a solicitação de adição de novas aplicações nas listas de controle de aplicativos através de interface web;

3.3.6.4. Oferecer proteção para chaves de registro e controle de processos;

3.3.6.5. Proibir através de política a inicialização de um processo ou aplicativo baseado em nome e no Hash do arquivo;

3.3.6.6. Detectar aplicativo controlado quando os usuários o acessarem, com as opções de permitir e alertar ou bloquear e alertar;

3.3.6.7. Deve possuir a opção de customizar uma mensagem a ser mostrada ao usuário em caso de bloqueio de execução do aplicativo;

3.3.6.8. Gerenciar o uso de dispositivos de armazenamento USB (ex: pen-drives e HDs USB). Permitir, através de regras, o bloqueio ou liberação da leitura/escrita/execução do conteúdo desses dispositivos;

3.3.6.9. Controlar o uso de outros dispositivos periféricos, como comunicação infravermelha e modem externo;

3.3.6.10. As funcionalidades do Controle de Aplicações e Dispositivos deverão ser nativas do produto ou incorporadas automaticamente por meio de plug-ins sem utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo fabricante;

3.3.6.11. Controle de vulnerabilidades do Windows e dos aplicativos instalados;

3.3.6.12. Capacidade de bloquear execução de aplicativo que está em armazenamento externo;

3.3.6.13. A gestão desses dispositivos deverá feita diretamente console de gerenciamento com a possibilidade de definir políticas diferentes por grupos de endpoints;

a) Permitir a autorização de um dispositivo com no mínimo as seguintes opções:

b) Permitir que todos os dispositivos do mesmo modelo;

c) Permitir que um único dispositivo com base em seu número de identificação único;

d) Permitir o acesso total;

e) Permitir acesso somente leitura;

3.3.7. **Funcionalidade de Proteção e Prevenção a Perda de Dados:**

3.3.7.1. Possuir proteção a vazamento ou perda de dados sensíveis, considerando o seu conteúdo ou o seu tipo real, além da possibilidade de avaliar a extensão do arquivo e múltiplos destinos como colocado abaixo;

3.3.7.2. Permitir a identificação de informações confidenciais, como números de passaportes ou outras informações pessoais identificáveis e/ou informações confidenciais mesmo que os documentos não tenham sido corretamente classificados, utilizando CCLs (Lista de Controle de Conteúdo);

3.3.7.3. Possibilitar o bloqueio, somente registrar o evento na Console de administração, ou perguntar ao usuário se ele ou ela realmente quer transferir o arquivo identificado como sensível;

3.3.7.4. Deve possuir listas de CCLs pré-configurados com no mínimo as seguintes identificações:

a) Números de cartões de crédito;

b) Números de identificação nacional, como CPF, RG, CNH;

c) Números de contas bancárias;

d) Números de Passaportes;

e) Endereços;

f) Números de telefone;

g) Códigos postais definidas por países como França, Inglaterra, Alemanha, EUA, etc;

h) Lista de e-mails;

3.3.7.5. Suportar adicionar regras próprias de conteúdo com um assistente

fornecido para essa finalidade;

3.3.7.6. Permitir criar regras de prevenção de perda de dados por tipo verdadeiro de arquivo.

3.3.7.7. Possuir a capacidade de autorizar, bloquear e confirmar a movimentação de dados sensíveis e em todos os casos, gravar a operação realizada com as principais informações da operação;

3.3.7.8. Permitir o controle de dados para no mínimo os seguintes meios:

a) Anexado no cliente de e-mail (ao menos Outlook e Outlook Express);

b) Anexado no navegador (ao menos IE, Firefox e Chrome);

c) Anexado no cliente de mensagens instantâneas (ao menos Skype);

d) Anexado a dispositivos de arma menos USB, CD/DVD);

3.4. CARACTERÍSTICAS GERAIS DA SOLUÇÃO DE PROTEÇÃO PARA SERVIDORES

3.4.1. **Características básicas do agente de proteção contra malwares:**

3.4.1.1. A solução deverá ser capaz de proteger servidores contra malwares, arquivos e tráfego de rede malicioso, controle de periféricos, controle de acesso à web, controle de aplicativos em um único agente instalado nos servidores;

3.4.1.2. O agente host deve buscar algum sinal de malwares ativos e detectar malwares desconhecidos;

3.4.1.3. O agente deve realizar a atualização várias vezes por dia para manter a detecção atualizada contra as ameaças mais recentes;

3.4.1.4. A solução deve manter conexão direta com banco de dados de ameaças do fabricante para uso da rede de inteligência;

3.4.1.5. Deve realizar a verificação de todos os arquivos acessados em tempo real, mesmo durante o processo de boot;

3.4.1.6. Deve realizar a verificação de todos os arquivos no disco rígido em intervalos programados;

3.4.1.7. Deve realizar a limpeza do sistema automaticamente, removendo itens maliciosos detectados e aplicações potencialmente indesejáveis (PUA);

3.4.1.8. Deve proteger os navegadores Internet Explorer, Firefox, Chrome, Opera e Safari, bloqueando o acesso a sites infectados conhecidos e pela verificação dos dados baixados antes de serem executados;

3.4.1.9. Deve permitir a autorização de detecções maliciosas e excluir da varredura diretórios e arquivos específicos;

3.4.1.10. É requerida a proteção integrada, ou seja, em um único agente, contra ameaças de segurança, incluindo vírus, spyware, trojans, worms, adware e aplicativos potencialmente indesejados (PUAs);

3.4.1.11. O cliente para instalação em estações de trabalho deverá ser compatível com os sistemas operacionais abaixo:

a) Windows Server 2016;

b) Windows Server 2012 R2 (64 bit);

c) Windows Server 2012 (64 bit);

d) Windows Server 2008 R2 (64 bit);

e) Windows Server 2008 (32 or 64 bit);

f) Amazon Linux;

g) CentOS;

h) Novell Open Enterprise Server 2015 SP1;

i) Oracle Linux 6.2/7;

j) Red Hat Enterprise Linux 6/7;

k) SUSE 11/12;

l) Ubuntu Server 14.04/16.04;

3.4.1.12. Deve suportar o uso de servidores usados para atualização em cache para diminuir a largura de banda usada nas atualizações;

3.4.1.13. Deve possuir integração com as nuvens da Microsoft Azure e Amazon Web Services para identificar as informações dos servidores instanciados nas nuvens;

3.4.1.14. Possuir a funcionalidade de proteção contra a alteração das configurações do agente, impedindo aos usuários, incluindo o administrador local, reconfigurar, desativar ou desinstalar componentes da solução de proteção;

3.4.1.15. Permitir a utilização de senha de proteção para possibilitar a reconfiguração local no cliente ou desinstalação dos componentes de proteção;

3.4.1.16. Deve possuir funcionalidades de monitoração de integridade de arquivos.

3.4.1.17. Deve possuir funcionalidades de whitelistening total do servidor, onde esta funcionalidade atue como um congelamento do servidor, não permitindo que novas aplicações sejam instaladas/executadas sem que seja previamente liberada pela console de gerenciamento da solução

3.4.1.18. Deve possuir funcionalidades de monitoramento do firewall local do Windows.

3.4.2. **Funcionalidade de Detecção e Proteção de Intrusão com as funcionalidades:**

3.4.2.1. Possuir proteção contra exploração de buffer overflow;

3.4.2.2. Possuir proteção contra ataques de Negação de serviço;

3.4.2.3. Deverá possui atualização periódica de novas assinaturas de ataque;

3.4.2.4. Capacidade de reconhecer e bloquear automaticamente as aplicações em clientes baseando-se na impressão digital (hash) do arquivo.

3.4.2.5. Capacidade de bloqueio de ataques baseado na exploração de vulnerabilidade conhecidas;

3.4.2.6. Detectar e bloquear técnicas de evasão, incluindo process injection e uso de executáveis legítimos do Windows para rodar scripts e ações maliciosas.

3.4.2.7. Possuir um sistema de prevenção de intrusão no host (HIPS), que monitore o código e blocos de código que podem se comportar de forma maliciosa antes de serem executados.

3.4.2.8. Ser capaz de aplicar uma análise adicional, inspecionando finalmente o comportamento de códigos durante a execução, para detectar comportamento

suspeito de aplicações, tais como buffer overflow.

3.4.2.9. Deve possuir técnicas de proteção, que inclui:

a) Análise dinâmica de código - técnica para detectar malware criptografado mais complexo;

b) Algoritmo correspondente padrão - onde os dados de entrada são comparados com um conjunto de sequências conhecidas de código já identificado como um vírus;

c) Emulação - uma técnica para a detecção de vírus polimórficos, ou seja, vírus que se escondem criptografando-se de maneira diferente cada vez que se espalham;

d) Tecnologia de redução de ameaças - detecção de prováveis ameaças por uma variedade de critérios, como extensões duplas (por exemplo .jpg .txt) ou a extensão não coincida com o tipo de arquivo verdadeiro (por exemplo, um arquivo executável ou arquivo .exe com a extensão .txt);

3.4.2.10. Verificação de ameaças web avançadas: bloqueia ameaças verificando o conteúdo em tempo real e remontando com emulação de JavaScript e análise comportamental para identificar e parar o código malicioso de malware avançados;

3.4.3. **Funcionalidade de Antivírus e AntiSpyware:**

3.4.3.1. Proteção em tempo real contra vírus, trojans, worms, rootkits, botnets, spyware, adwares e outros tipos de códigos maliciosos.

3.4.3.2. Proteção anti-malware deverá ser nativa da solução ou incorporada automaticamente por meio de plug-ins sem a utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo fabricante.

3.4.3.3. As configurações do anti-spyware deverão ser realizadas através da mesma console do antivírus;

3.4.3.4. Permitir a configuração de ações diferenciadas para programas potencialmente indesejados ou malware, com possibilidade de inclusão de arquivos em listas de exclusão (whitelists) para que não sejam verificados pelo produto;

3.4.3.5. Permitir a varredura das ameaças da maneira manual, agendada e em tempo real nos servidores;

3.4.3.6. Capacidade de detecção e reparo em tempo real de vírus de macro conhecidos e novos através do antivírus;

3.4.3.7. Capacidade de detectar arquivos através da reputação dos mesmos;

3.4.3.8. Capacidade de remoção automática total dos danos causados por spyware, adwares e worms, como limpeza do registro e pontos de carregamento, com opção de finalizar o processo e terminar o serviço da ameaça no momento de detecção;

3.4.3.9. A remoção automática dos danos causados deverá ser nativa do próprio antivírus; ou adicionada por plugin, desde que desenvolvido ou distribuído pelo fabricante;

3.4.3.10. Capacidade de bloquear origem de infecção através de compartilhamento de rede com opção de bloqueio da comunicação via rede;

3.4.3.11. Deverá detectar tráfego de rede para comandar e controlar os servidores;

3.4.3.12. Proteger arquivos de documento contra ataques do tipo ransomwares;

3.4.3.13. Proteger que o ataque de ransomware seja executado remotamente;

3.4.3.14. Permitir o envio de amostras de malwares para a nuvem de inteligência do fabricante;

3.4.3.15. Permitir o bloqueio da verificação de vírus em recursos mapeados da rede;

3.4.3.16. Antivírus de Web (verificação de sites e downloads contra vírus);

3.4.3.17. Controle de acesso a sites por categoria;

3.4.3.18. Proteger a navegação na web, mesmo aos usuários fora da rede, para todos os principais navegadores (IE, Firefox, Safari, Opera e Chrome), fornecendo controle da Internet independentemente do browser utilizado sem utilizar um plugin, onde não é possível ser ignorada pelos usuários, protegendo os usuários de websites infectados e categorias específicas de websites.

3.4.3.19. O Controle da Web deve controlar o acesso a sites impróprios, com no mínimo 14 categorias de sites inadequados. Deve ainda permitir a criação de lista branca de sites sempre permitidos e lista negra de sites que devem ser bloqueados sempre;

3.4.3.20. Todas as atividades de navegação na Internet bloqueadas deverão ser enviadas para a console de gerenciamento, informando detalhes do evento e a razão para o bloqueio;

3.4.3.21. Capacidade de verificar somente arquivos novos e alterados;

3.4.3.22. Funcionalidades específicas para prevenção contra a ação de ransomwares, tais como a capacidade de impedir a criptografia quando feita por aplicativos desconhecidos ou a capacidade de fazer backup de arquivos antes de serem criptografados para posteriormente permitir sua restauração.

3.4.3.23. Capacidade de habilitar mensagens de desktop para a Proteção contra Ameaças;

3.4.3.24. Capacidade de adicionar exclusão de varredura para arquivos, pastas, processos, sites, aplicativos e tipos de explorações detectadas;

3.4.4. **Funcionalidade de proteção contra ransomwares:**

3.4.4.1. Deve dispor de capacidade de proteção contra ransomware não baseada exclusivamente na detecção por assinaturas;

3.4.4.2. Deve dispor de capacidade de remediação da ação de criptografia maliciosa dos ransomwares;

3.4.4.3. Deve dispor de capacidade de prevenção contra a ação de criptografia maliciosa executada por ransomwares, possibilitando ainda o bloqueio dos computadores de onde partirem tal ação;

3.4.4.4. Deverá ser capaz de remover o ranswonware do computador sem que o usuário perca nenhum arquivo, utilizando técnicas de backup e rollback com eficiência o suficiente para que não se percam arquivos;

3.4.5. **Funcionalidade de Controle de aplicações e dispositivos:**

3.4.5.1. Possuir controle de aplicativos para monitorar e impedir que os usuários executem ou instalem aplicações que podem afetar a produtividade ou o

desempenho da rede;

3.4.5.2. Atualiza automaticamente a lista de aplicativos que podem ser controlados, permitindo que aplicativos específicos ou categorias específicas de aplicações possa ser liberada ou bloqueada;

3.4.5.3. Verificar a identidade de um aplicativo de maneira genérica para detectar todas as suas versões. Permitir a solicitação de adição de novas aplicações nas listas de controle de aplicativos através de interface web;

3.4.5.4. Oferecer proteção para chaves de registro e controle de processos;

3.4.5.5. Proibir através de política a inicialização de um processo ou aplicativo baseado em nome e no Hash do arquivo;

3.4.5.6. Detectar aplicativo controlado quando os usuários o acessarem, com as opções de permitir e alertar ou bloquear e alertar;

3.4.5.7. Deve possuir a opção de customizar uma mensagem a ser mostrada ao usuário em caso de bloqueio de execução do aplicativo;

3.4.5.8. Gerenciar o uso de dispositivos de armazenamento USB (ex: pen-drives e HDs USB). Permitir, através de regras, o bloqueio ou liberação da leitura/escrita/execução do conteúdo desses dispositivos;

3.4.5.9. Controlar o uso de outros dispositivos periféricos, como comunicação infravermelha e modem externo;

3.4.5.10. As funcionalidades do Controle de Aplicações e Dispositivos deverão ser nativas do produto ou incorporadas automaticamente por meio de plug-ins sem utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo fabricante;

3.4.5.11. Controle de vulnerabilidades do Windows e dos aplicativos instalados;

3.4.5.12. Capacidade de bloquear execução de aplicativo que está em armazenamento externo;

3.4.5.13. A gestão desses dispositivos deverá feita diretamente console de gerenciamento com a possibilidade de definir políticas diferentes por grupos de endpoints;

3.4.5.14. Permitir a autorização de um dispositivo com no mínimo as seguintes opções:

a) Permitir que todos os dispositivos do mesmo modelo;

b) Permitir que um único dispositivo com base em seu número de identificação único;

c) Permitir o acesso total;

d) Permitir acesso somente leitura;

3.4.6. **Funcionalidade de Proteção e Prevenção a Perda de Dados:**

3.4.6.1. Possuir proteção a vazamento ou perda de dados sensíveis, considerando o seu conteúdo ou o seu tipo real, além da possibilidade de avaliar a extensão do arquivo e múltiplos destinos como colocado abaixo;

3.4.6.2. Permitir a identificação de informações confidenciais, como números de passaportes ou outras informações pessoais identificáveis e/ou informações confidenciais mesmo que os documentos não tenham sido corretamente

classificados, utilizando CCLs (Lista de Controle de Conteúdo);

3.4.6.3. Possibilitar o bloqueio, somente registrar o evento na Console de administração, ou perguntar ao usuário se ele ou ela realmente quer transferir o arquivo identificado como sensível;

3.4.6.4. Deve possuir listas de CCLs pré-configurados com no mínimo as seguintes identificações:

- Números de cartões de crédito;
- Números de contas bancárias;
- Números de Passaportes;
- Endereços;
- Números de telefone;
- Códigos postais definidas por países como França, Inglaterra, Alemanha, EUA, etc;
- Lista de e-mails;

3.4.6.5. Suportar adicionar regras próprias de conteúdo com um assistente fornecido para essa finalidade;

3.4.6.6. Permitir criar regras de prevenção de perda de dados por tipo verdadeiro de arquivo.

3.4.6.7. Possuir a capacidade de autorizar, bloquear e confirmar a movimentação de dados sensíveis e em todos os casos, gravar a operação realizada com as principais informações da operação;

3.4.6.8. Permitir o controle de dados para no mínimo os seguintes meios:

- Anexado no cliente de e-mail (ao menos Outlook e Outlook Express);
- Anexado no navegador (ao menos IE, Firefox e Chrome);
- Anexado no cliente de mensagens instantâneas (ao menos Skype);
- Anexado a dispositivos de armazenamento (ao menos USB, CD/DVD);

3.5. SEGURANÇA DE MENSAGERIA

3.5.1. 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;

3.5.2. 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;

3.5.3. A licença de uso deve atingir um número de 750 (setecentos e cinquenta) caixas postais;

3.5.4. 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;

3.5.5. Deve permitir alta disponibilidade das funções de filtragem, de maneira assegurar que o serviço de correio nunca pare por falha da solução;

3.5.6. A solução deve suportar o processamento de no mínimo 20.000 (dez mil) conexões simultâneas e 160.000 (cento e sessenta mil) mensagens por hora;

3.5.7. Deve ser capaz de efetuar implantação em appliance virtual, para expansão da solução de hardware a qualquer tempo, sem cobrança adicional de licença ou limitação de appliance virtual, sendo compatível com os principais sistemas

de virtualização do mercado, entre eles:

a) VMWare;

b) Microsoft Hyper-V.

3.5.8. **Pontos Gerais:**

3.5.8.1. A licença de uso do software deve possuir 12 (doze) meses de atualização do fabricante compreendendo os seguintes módulos:

3.5.8.2. 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;

3.5.8.3. 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;

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

3.5.8.5. Analisar mensagens, no mínimo, por meio dos seguintes métodos:

- Proteção dinâmica por reputação;
- Assinaturas de spam;
- 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 dois módulos de antivírus, sendo um do próprio fabricante, já devidamente licenciado para uso simultâneo;

- Filtros de anexos;
- Filtros de phishing;
- Análise heurística;
- Análise do cabeçalho, corpo e anexo das mensagens;
- E-mail bounce;
- Dicionários pré-definidos e customizados com palavras e expressões regulares;

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

- Número de cartão de crédito;
- CNPJ;
- RG e CPF;

3.5.8.7. Deve possuir mecanismo de backup e recuperação da configuração da solução;

3.5.8.8.

3.5.8.9. 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).

3.5.8.10. Os manuais necessários à instalação e administração da solução, devem constar no seguinte idioma: Português do Brasil ou Inglês;

3.5.8.11. A interface de administração do sistema deve ter suporte a no mínimo um dos seguintes idiomas:

- Português do Brasil;
- Inglês.

3.5.8.12. A interface de quarentena do usuário deve suportar o idioma Português do Brasil;

3.5.8.13.

3.5.8.14. 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;

3.5.8.15. Deve possuir capacidade de configuração de roteamento de mensagens para múltiplos domínios de destino;

3.5.8.16. Deve permitir a configuração de múltiplos domínios, com aplicação de regras de forma independente para cada um dos domínios;

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

3.5.8.18. 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 appliance se o administrador assim desejar;

3.5.8.19. A solução deve permitir criação de regras por:

- Grupos de usuários;
- Domínios;
- Range de IP;
- IP/Rede;
- Remetentes específicos;
- Destinatários específicos;
- Grupos de LDAP.

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

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

3.5.8.22. 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”;

3.5.8.23. A console de gerenciamento deve acessada através de protocolo seguro (HTTPS – HyperText Transfer Protocol Secure) com no mínimo as seguintes funcionalidades:

3.5.8.24. Administração centralizada de todas as regras e filtros integrantes da

solução;

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

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

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

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

3.5.8.29. Deve possuir administração via shell, através de SSH para CLI (command line interface), para execução de comandos de administração e suporte;

3.5.8.30. Deve ser capaz de utilizar os protocolos de transferência de arquivos SCP e FTP;

3.5.8.31. Suporte à assinatura e validação de autenticidade de mensagens através de Domains Keys, DKIM e SPF;

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

- Conteúdo do anexo;
- Mime-Type do anexo;
- Extensão do anexo;
- Nome completo do anexo;
- Nome parcial do anexo;
- Expressão regular;
- Tamanho do anexo;
- Anexos compactados com senha;
- Quantidade de níveis de compactação no mesmo anexo.

3.5.8.33. Deve possuir um sistema de Disaster e Recovery ao qual é efetuado o upload de um arquivo de backup e restauração do mesmo automaticamente;

3.5.8.34. 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.

3.5.8.35. Deve possuir sistema de diagnóstico via interface WEB, com no mínimo a execução dos seguintes testes:

3.5.8.36. Teste de Conectividade TCP – Informando o Host e a Porta a serem testados;

- Teste de Conectividade ICMP – Informando o Host a ser testado;
- Teste de DNS – Informando o Host ou o Domínio a serem testados;
- Teste de Envio de E-mail;
- Teste de Lookup de E-mail via LDAP;
- Teste de Conectividade com o fabricante (para isso, testa-se as portas necessárias de comunicação junto ao fabricante);
- Teste de TRACEROUTE;
- Teste de DNS Reverso;
- Teste de SPF, para checar se tem registro para um determinado domínio;
- Teste de DKIM, para checar se tem registro para um domínio;
- Teste de DMARC, para checar se tem registro para um domínio;
- Teste de portas de Saída utilizadas pelo sistema.

3.5.8.37. 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:

- Serviço de antivírus;
- Serviço de MTA;
- Serviço de Banco de Dados;
- Serviço de SMNP.

3.5.8.38. Deve permitir a instalação de agentes/plug-ins (tanto no appliance de gerenciamento, quanto nos agentes que fazem a filtragem) para monitoramento com sistemas de terceiros, com no mínimo:

- Zabbix;
- Nagios.

3.5.9. **Da alta disponibilidade:**

3.5.9.1. 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;

3.5.9.2. Deve permitir a configuração em Cluster com appliances físicos ou virtualizados em DataCenters distintos;

3.5.9.3. O cluster deve poder ser formado por appliances físicos e appliances virtuais de forma mista.

3.5.9.4. 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;

3.5.9.5. 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;

3.5.9.6. Possuir capacidade de replicação automática das configurações e balanceamento de carga através um único Virtual IP.

3.5.10. **Do Gerenciamento:**

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

3.5.10.2. 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, sendo possível definir quais endereços de e-mails ou domínios ele poderá auditar;

3.5.10.3. O sistema deve possuir ainda, no mínimo, os perfis pré-definidos:

- Administrador: Com acesso total às configurações da solução;
- Administrador: Com acesso total às configurações da solução sem acesso à leitura dos e-mails armazenados tanto na quarentena como mensagens auditadas;
- Auditor: Com acesso a visualização dos e-mails armazenados para auditoria;
- Operador: Com acesso à administração da quarentena e gerenciamento da “Black e White List”;

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

3.5.10.4. Permitir a criação de grupos, para posterior aplicação de regras. Os grupos poderão ser criados através das seguintes métricas:

- E-mails;
- Domínios;
- IP’s;
- Range de IP;
- Expressão Regular;
- Usuários;
- Listas de distribuição;
- Grupos de LDAP.

3.5.11. **Alertas e logs da solução:**

3.5.11.1. Deve enviar notificações por e-mail ao administrador, caso as atualizações não tenham sido realizadas com sucesso;

3.5.11.2. A solução deve ser capaz de gerar notificações a remetente e/ou destinatário com mensagem de alerta customizável;

3.5.11.3. 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;

3.5.11.4. Possuir mecanismo de alerta por e-mail quando houver nova atualização do sistema e sobre o status do processo de atualizações;

3.5.11.5. 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:

- Emergency;
- Alert;
- Critical;
- Error;
- Warning;
- Notice;
- Informational;
- Debug.

3.5.11.6. Deve ser possível enviar alertas por e-mail e por snmp caso ocorra consumo excessivo de algum recurso do sistema. Os sistemas monitorados para envio dos alertas devem ser, no mínimo:

- Espaço em disco;
- Filas de e-mail;
- Memória;
- Processador;
- Serviço de Filtragem;
- Atualização do sistema de segurança;
- Antivírus e Antispam;
- Ponto de acesso indisponível.

3.5.12. **Das Funcionalidades para o Usuário Final:**

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

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

- Português do Brasil.

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

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

3.5.12.5. 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;

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

- Português do Brasil.

3.5.13. **Da quarentena:**

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

3.5.13.2. 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;

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

3.5.13.4. A interface deve permitir identificar quais Regras do Módulo de AntiSpam foram ativadas e qual sua pontuação, a fim de permitir ao administrador a elaboração de regras granulares;

3.5.13.5. A solução deve suportar a criação de áreas de quarentena personalizadas para usuários específicos;

3.5.13.6. Deve permitir também que todas as áreas de quarentenas sejam armazenadas de forma criptografadas no próprio appliance, seja ele virtual ou físico.

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

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

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

3.5.13.10. 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;

3.5.13.11. O tempo de armazenamento da quarentena deve ser individual por área de quarentena, devendo também permitir armazenamento por tempo "indeterminado";

3.5.13.12. Possibilitar ao administrador selecionar o rotacionamento das mensagens em quarentena por tamanho da quarentena, por exemplo limitar uma quarentena a 100GB, sendo que ao ultrapassar o limite deste tamanho, o sistema automaticamente começará a apagar os e-mails quarentenados mais antigos;

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

3.5.13.14. Pelo sigilo da informação, permitir que seja selecionada quais quarentenas customizadas somente sejam acessíveis a determinados administradores, permitindo a granularidade de acesso destas quarentenas.

3.5.14. **Dos Usuários e Grupos:**

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

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

3.5.14.3. 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;

3.5.14.4. 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;

3.5.14.5. Integração nativa com o Microsoft Exchange;

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

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

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

3.5.15. **Dos relatórios:**

3.5.15.1. Deve permitir a geração de relatórios de todos os appliances de um cluster de forma centralizada através de uma única interface web no console de gerenciamento;

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

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

3.5.15.4. Deve ser possível configurar um período para a retenção dos dados utilizados para geração dos relatórios;

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

- Sumário de mensagens;
- Quantidade de mensagens processadas;
- Relatório de Volume de Mensagens por Data;
- Principais origens de spam por domínio, endereço de e-mail;
- Principais destinos de spam por domínio, endereço de e-mail;
- Principais origens de vírus;
- Principais fontes de ataque;
- Relatório de Top E-mail Relays;
- Relatório de Top Remetentes por Quantidade;
- Relatório de Top Remetentes por Volume;
- Relatório de Top Destinatário por Quantidade;
- Relatório de Top Destinatário por Volume;
- Estatísticas da quarentena;
- Conexões completadas X bloqueadas;
- Relatório de tráfego;
- Principais destinatários de Spam;
- Principais destinatários de e-mail;
- Top Ataques por fraude de e-mail / tentativa de spoof.
- Permitir filtros de relatórios com definição de origem e destinos específico;
- Possuir relatórios estatísticos de conexões, ameaças, quarentena e SPAM;
- Deve apresentar estatísticas e monitoramento em tempo real (online) de e-mails com base em gráficos;
- Os relatórios, no mínimo, devem poder ser filtrados por:
- Período de tempo;
- Ponto de Filtragem que o e-mail passou;
- De;
- Para;
- Qual a classificação que a mensagem atingiu, dentre eles no mínimo:
- DLP;
- Provável SPAM;
- SPAM;
- Vírus;
- Conteúdo Bloqueado;
- Whitelist;
- Blacklist;
- Tamanho Excedido;
- Phishing.
- Relatório para um único usuário ou Domínio.

3.5.16. **Rastreamento das mensagens:**

3.5.16.1. 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);

3.5.16.2. O rastreamento deve ser possível através de qualquer um dos seguintes

campos:

- ID da mensagem;
- E-mail do Remetente;
- E-mail do Destinatário;
- Domínio do Remetente;
- Domínio do Destinatário;
- Assunto da mensagem;
- Nome do anexo;
- Palavra contida no conteúdo do corpo da mensagem;
- IP de Origem da mensagem;
- Tamanho da mensagem;
- Regra de SPAM;
- Regra de DLP;
- Se a mensagem foi entregue ou não;
- Regras personalizadas aplicadas na mensagem;
- Nome da ameaça encontrada.

3.5.16.3. 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 appliance 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:

- Remetente da mensagem;
- Destinatários da mensagem;
- Servidor de origem;
- Se foi armazenada em quarentena;
- Se continha vírus;
- A regra que atuou;
- O servidor de origem;
- O tamanho da mensagem;
- Se foi entregue ou não;
- Qual ponto de filtragem utilizado (qual appliance 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.

3.5.17. **Proteção contra ataques direcionados:**

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

3.5.17.2. Ser uma solução MTA (Mail Transfer Agent) completa suportando o protocolo SMTP, e com Suporte a envio e recebimento de e-mails criptografados utilizando o protocolo TLS/ SSL, permitindo configurar domínios onde o TLS é mandatório;

3.5.17.3. A solução deverá possuir a capacidade de executar as seguintes ações:

3.5.17.4. Limitar o número de conexões TCP permitidas através de um valor configurável;

3.5.17.5. Rejeitar a conexão SMTP que se caracterize como "flooding".

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

- Vírus;
- Spyware;
- Worms;
- Trojans;
- Spam;
- Phishing;
- E-mail Marketing, ou qualquer outra forma de ameaça virtual.

3.5.17.7. Deve possuir controle total da comunicação permitindo restringir:

- IP reverso mal configurado;
- Domínios inexistentes;
- Permitir identificar e bloquear e-mails vindos de domínios recentemente cadastrados.

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

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

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

- Aceitar;
- Colocar em quarentena;
- Inserir tag personalizada no assunto;
- Marcar o cabeçalho.

3.5.17.11. A solução deve ser capaz de tomar as seguintes ações sobre as

mensagens:

- Alterar o assunto da mensagem;
- Adicionar cabeçalhos para rastreamento;
- Descartar a mensagem;
- Colocar em uma determinada área de quarentena definida pelo administrador.

3.5.17.12. Deve permitir a criação de regras baseadas no idioma que as mensagens foram escritas, com capacidade de identificar no mínimo, português, inglês e espanhol;

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

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

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

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

3.5.17.17. 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;

3.5.17.18. 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”;

3.5.17.19. 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:

- IP reverso e localização;
- Registro em blacklists mundiais;
- Configuração de serviço de notificação de envio e autenticidade de mensagens de mensagens como SPF e DKIM.

3.5.17.20. 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;

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

3.5.17.22. 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 do appliance, em especial baseado em lista local de bloqueio de conexão por: IP, e-mail, domínio, RBL’s e SPF;

3.5.17.23. Deve permitir que o administrador do sistema cadastre novas RBL’s para serem utilizadas a nível de conexão SMTP;

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

3.5.17.25. 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;

3.5.17.26. Possuir mecanismo de “Spam Throttling” permitindo ao administrador limitar o fluxo de mensagens recebidas de origens com baixa reputação;

3.5.17.27. 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;

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

3.5.17.29. Possuir controle de “Outbreak”, penalizando o remetente por um tempo configurável pelo administrador ao detectar:

3.5.17.30. Número excessivo de spams (configurado pelo administrador) oriundos de uma mesma fonte de e-mail;

3.5.17.31. Número excessivo de vírus (configurado pelo administrador) oriundos de uma mesma fonte de e-mail;

3.5.17.32. Número excessivo de ataques de dicionário (configurado pelo administrador) oriundos de uma mesma fonte de e-mail;

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

- Fontes de ataques;
- Ameaças encontradas.

3.5.18. **Da proteção contra SPAM e PHISHING:**

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

- FingerPrint: Filtro por assinatura de spam;
- Análise Heurística: Análise completa de toda mensagem contra spam, de acordo com as características da mensagem;
- Análise de Documentos: Análise de documentos anexados na mensagem (PDF, DOC, DOCX e TXT);
- Análise de Imagens: Filtragem de spam em imagens;
- Filtro de URL: Filtragem por URL mal-intencionada contidas no corpo da mensagem, dessa forma combatendo possível e-mail Phishing;

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

- Conteúdo pornográfico;
- Abuso infantil;
- Redes sociais;
- Racismo e ódio;
- Pesquisa de empregos;
- Streaming de áudio;
- Streaming de vídeo;
- Esportes;
- Notícias;

- Compras Online.

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

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

3.5.18.5. 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;

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

- Recurso de Grey List;
- 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";
- Recurso de checagem por DMARC;
- Recurso de checagem por assinatura DKIM;
- Recurso de checagem de DNS Reverso;
- Checagem de validade de domínio através de verificação da configuração da zona do DNS do remetente;
- Análise de reputação de IP;
- Reputação de Mensagens;
- Filtros de URL;
- Filtro de anti-phishing;
- Consulta de RBL´s (real-time blackhole list);
- Machine Learning.

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

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

- Origens das mensagens;
- Destino das mensagens;
- Domínios;
- Endereços de e-mails;
- Expressões regulares (dicionário de palavras);
- Fluxo;
- Quantidade de mensagens;
- Tamanho de anexo;
- Número máximo de destinatários em uma única mensagem;

- Tipo de arquivos em anexo;
- Extensões de arquivos em anexo, identificados por Mime-Type;
- Anexos criptografados;
- Anexos compactados;
- Níveis de compactação dos arquivos anexos;
- Quantidade de anexos na mensagem;
- Conteúdo HTML no corpo da mensagem.

3.5.18.9. 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:

- "<form>";
- "<script>";
- "<iframe>".

3.5.18.10. 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:

- Entregar direto o e-mail;
- Colocar em quarentena;
- Remover mensagem;
- Auditar mensagem;
- Encaminhar a mensagem;
- Notificar o destinatário;
- Adicionar header na mensagem;
- Transformar HTML em texto simples.

3.5.18.11. 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;

3.5.18.12. 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;

3.5.18.13. 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;

3.5.18.14. 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;

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

3.5.18.16. Possuir proteção contra bounce e-mail attack através "Bounce Address Tag Verification";

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

3.5.18.18. 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;

3.5.18.19. 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:

- Microsoft Exchange.

3.5.19. **Da proteção contra VÍRUS:**

3.5.19.1. Possuir módulo de verificação com suporte a dois ou mais mecanismos diferentes de antivírus, executando simultaneamente;

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

3.5.19.3. Scan de arquivos compactados recursivamente, no mínimo, 5 (cinco) camadas, contemplando no mínimo, os seguintes compactadores: .rar, .zip, .tar, .arj, .cab, .lha, .exe, .lzh, .tgz e .gzip;

3.5.19.4. A solução deve possuir, no mínimo, duas engines de antivírus e antimalware já integrados na solução sem custo adicional;

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

- Dia-zero (zero-day);
- Vírus outbreak;
- Hora-zero (Zero-hour);
- Targeted Attack Protection;
- APT - advanced persistent threat.

3.5.19.6. Tomar no mínimo as seguintes ações:

- Descartar a mensagem;
- Colocar em uma determinada área da quarentena definida pelo administrador.

3.5.19.7. **Das notificações de quarentena individual do usuário:**

3.5.19.8. A solução deverá permitir ao administrador agendar o envio do resumo das mensagens na quarentena individual do usuário (digest) em períodos de tempo pré-configurável 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;

3.5.19.9. Grupos diferentes de usuários devem poder receber a notificação em horários diferentes;

3.5.19.10. 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;

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

- E-mail de origem;
- Título/Assunto do e-mail;

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

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

- Liberar uma mensagem bloqueada;

3.5.19.13. Bloquear o remetente da mensagem (blacklist), para que as futuras mensagens do mesmo já sejam barradas;

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

3.5.19.15. Reportar o bloqueio indevido;

3.5.19.16. Solicitar envio de novo resumo;

3.5.19.17. Acessar sua área de quarentena;

3.5.19.18. 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);

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

- Liberar e-mail;
- Reportar Falso Positivo;
- 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;

3.5.20. **Do disclaimer:**

3.5.20.1. Capacidade de incluir “disclaimers” nas mensagens enviadas;

3.5.20.2. 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 Directory;

3.5.20.3. A solução deverá suportar a configuração dos “disclaimers” em formato html e texto.

3.5.21. **Prevenção a roubo de informação (DLP) e Compliance:**

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

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

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

- Identificação de CPF;
- Número de cartão de crédito;
- CNPJ.

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

- Cabeçalho;
- URL (contidas no e-mail);
- Corpo do e-mail;
- Anexos e documentos no mínimo: .DOC, .DOCX, .XLS, .XLSX, .PDF, .PPT, .PPTX e .TXT.

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

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

- Entregar a mensagem;
- Não entregar a mensagem;
- Armazenar a mensagem para auditoria;
- Notificar remetente e destinatário da mensagem;
- Encaminhar a mensagem para outro destinatário.

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

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

3.5.22. **Criptografia de E-mail:**

3.5.22.1. 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;

3.5.22.2. 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;

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

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

- Assunto;
- Destinatário;
- E-mail do Remetente;
- Nome do Anexo.

3.5.22.5. A criptografia das mensagens deve utilizar sistema de chaves gerada de forma independente;

3.5.22.6. Deve impossibilitar o uso de Cache de Browser para acesso às mensagens criptografadas;

3.5.22.7. Deve possibilitar ao administrador a indicação do tempo de expiração da mensagem criptografada;

3.5.22.8. Deve possibilitar ao administrador indicar se o destinatário poderá responder o e-mail;

3.5.22.9. Deve possibilitar ao administrador indicar se o destinatário poderá encaminhar o e-mail.

3.5.23. **Do Sistema de Proteção Contra Ataques Dirigidos (Targeted Attack Protection - TAP):**

3.5.23.1. Deverá prover proteção contra ataques dirigidos tais como:

- Spear-phishing;
- Ataques Zero-Day;
- Ameaças avançadas persistentes (APTs).

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

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

- Verificação da lista de códigos maliciosos: Verificação de campanhas de e-mails emergentes e conhecimento de novos sites maliciosos;
- Análise Estática (Análise de código): Verificação de comportamento suspeito, scripts escondidos, partes de códigos maliciosos e redirecionamento a outros sites maliciosos;
- Análise Dinâmica: Utilização de “Sandbox” para simular a máquina de um usuário real e observar as alterações efetuadas no sistema.

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

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

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

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

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

3.5.23.8. Deve ser possível habilitar ou desabilitar a proteção URL baseada em

rotas específicas configuradas no mínimo pelas seguintes condições:

- E-mail do Destinatário;
- E-mail do Remetente;
- Domínio de Origem;
- Domínio de Destino;
- IP/Rede;
- Range de IP;
- Expressão Regular;
- Usuários;
- Listas de distribuição;
- Grupo de LDAP.

3.5.23.9. 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;

3.5.23.10. O sistema deverá ser capaz de varrer anexos, com no mínimo, tipos PDF, arquivos em Flash para payloads maliciosos e microsoft office;

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

3.5.23.12. Deve possuir tecnologia SandBox local do mesmo fabricante ou 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);

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

3.5.23.14. 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;

3.5.23.15. A proteção URL deverá reescrever links para os protocolos HTTP, HTTPS, FTP e URL's que comecem com “www” independente do protocolo;

3.5.23.16. 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;

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

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

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

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

- 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;
- Bloqueado - Número de vezes que o módulo de Proteção URL impediu o usuário de acessar o site malicioso;
- Permitida – Número de vezes que o módulo de proteção URL permitiu ao usuário acessar o site original da URL reescrita e que não foi detectada como maliciosa.

3.5.23.21. O Dashboard deverá exibir timeline das ameaças, exibindo quando foi recebida, identificada e quando foi clicada ou liberada;

3.5.23.22. 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;

3.5.23.23. O Dashboard deverá possuir ferramenta para bloqueio ou liberação de URL pelo administrador da ferramenta;

3.5.23.24. 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;

3.5.23.25. O Dashboard deverá disponibilizar sistema de coleta (report) de amostra do IP para análise da engenharia do fabricante;

3.5.23.26. O Dashboard deverá possuir ferramenta para bloqueio ou liberação do IP pelo administrador da ferramenta;

3.5.23.27. 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

3.5.23.28. O Dashboard deverá possuir ferramenta para bloqueio ou liberação do arquivo pelo administrador da ferramenta;

3.5.23.29. 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;

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

- JavaScript;
- Links;
- Executáveis;
- VB Script.

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

- pdf;
- doc;
- docx;
- ppt;
- pptx;
- xls;

- xlsx.

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

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

- .swf;
- .pdf;
- .doc;
- .xls;
- .xlsx;
- .ppt;
- .ppt;
- .pptx;
- .rtf.

3.5.23.34. 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;

3.5.23.35. Deve poder desativar a reescrita de URL's se a mensagem atingir uma pontuação mínima de SPAM definida pelo administrador;

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

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

3.5.24. **Do Sistema de Proteção a Fraudes de E-mail:**

3.5.24.1. 5.25.1 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:

- Pontuar;
- Ignorar;
- Bloquear.

3.5.24.2. 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:

- Pontuar;
- Ignorar;
- Bloquear.

3.5.24.3. 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;

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

3.5.24.5. 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.

4. CONDIÇÕES DE MANUTENÇÃO

4.1. Manutenção e assistência técnica do tipo corretiva, compreendendo procedimentos destinados à recolocar em perfeito estado de operação os serviços e o objeto tais como:

a) Do hardware (nos casos de fornecimento de appliance): desinstalação, reconfiguração ou reinstalação decorrentes de falhas no hardware, fornecimento de peças de reposição, substituição de hardware, atualização da versão de drivers, firmwares e so ware básico, correção de defeitos, ajustes e reparos necessários, de acordo com os manuais e as normas técnicas específicas para os recursos u lizados;

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

4.2. Quanto às atualizações pertinentes aos softwares, entende-se como “atualização” o provimento de toda e qualquer evolução de software, incluindo correções, “patches”, “fixes”, “updates”, “service packs”, novas “releases”, “versions”, “builds”, “upgrades”, englobando inclusive versões não sucessivas, nos casos em que a liberação de tais versões ocorra durante o período de garantia especificado;

4.3. A manutenção e assistência técnica corretiva serão realizadas sempre que solicitada pela CONTRATANTE por meio da abertura de chamado técnico diretamente à empresa CONTRATADA (ou a sua Credenciada) via telefone (com número do tipo “0800” caso a Central de Atendimento esteja fora do Rio de Janeiro/RJ), Internet, e-mail, sem ônus;

4.4. A abertura de chamados pelo CONTRATANTE por correio eletrônico, será por sistema de controle de chamados, com email de resposta do chamado aberto apresentando o número do ticket aberto, para acompanhamento.

4.5. As respostas do suporte técnico contratado deverão ser efetuadas na língua portuguesa (português do Brasil), tanto por email, quanto por contato telefônico.

4.6. O prazo de atendimento começa a ser contado a partir da hora do acionamento do chamado técnico, através de telefone ou e-mail;

4.7. Um chamado técnico somente poderá ser fechado após confirmação de responsável da CONTRATANTE e o término de atendimento se dará com a disponibilidade do recurso para uso em perfeitas condições de funcionamento no local onde o mesmo está instalado;

4.8. A prioridade de atendimento dos chamados será definida pela CONTRATANTE;

4.9. Na abertura de chamados técnicos, serão fornecidas informações, como nome do produto, part number/serial number ou equivalente, anormalidade observada, nome do responsável pela solicitação do serviço e versão do software utilizada e severidade do chamado.

4.10. Todas as solicitações feitas pela CONTRATANTE deverão ser registradas

pela CONTRATADA em sistema informatizado para acompanhamento e controle da execução dos serviços e ainda:

4.10.1. A CONTRATADA após a realização dos serviços de garantia deverá apresentar um Relatório de Visita, contendo identificação do chamado, data e hora de abertura do chamado, data e hora do início e término do atendimento, identificação do defeito, técnico responsável pela solução, as providências adotadas e outras informações pertinentes. Este relatório deverá ser homologado por responsável do CONTRATANTE;

4.10.2. O tempo do início de atendimento do chamado técnico deverá ser de acordo com a Tabela de Severidade de Chamado e contado a partir da hora de abertura do chamado. Ou seja, a partir da hora de abertura do chamado, iniciada a contagem de tempo para o início do atendimento;

4.10.3. Após o início do atendimento, o tempo de solução do problema deverá ser de acordo com a tabela de solução do chamado, não devendo ultrapassar os prazos estabelecidos para as respectivas severidades, contados a partir da abertura do chamado técnico;

4.11. os níveis de atendimento serão conforme abaixo indicado:

TABELA DE SOLUÇÃO DO CHAMADO			
Severidade	**Descrição**	**Métrica**	**Atendimento**
1 - Alta	Quando há indisponibilidade de uso da solução	Prazo em horas úteis	Atendidos em até 1 (uma) hora após a abertura e deverão ser solucionados em até 24 (vinte e quatro) horas a partir da abertura do chamado.
2 - 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	Prazo em horas úteis	Atendidos em até 4 (quatro) horas após a abertura e deverão ser solucionados em até 48 (quarenta e oito) horas a partir da abertura do chamado.
3 - Baixa	Nível de severidade aplicado para instalação, configuração, atualização de versões e implementações de novas funcionalidades	Prazo em horas úteis	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.
4 - Informativo	Nível informacional ou dúvidas	Prazo em horas úteis	Nível informacional ou dúvidas

5. DA GARANTIA

5.1. O prazo de garantia contratual dos bens para o **Grupo I (Itens 1 e 2) será de, 36 (trinta e seis) meses** e para o **Item 3 será de 12 (doze) meses**,contado a partir do primeiro dia útil subsequente à data de assinatura do contrato.

5.2. Os prazos informados nos subitem 5.1 referem-se ao prazo estipulado para a assinatura das referidas licenças.

5.3. O suporte técnico e a garantia deverão ser prestados obrigatoriamente

quando ocorrer indisponibilidade de qualquer uma das soluções.

5.4. Durante o período de vigência da garantia, a CONTRATANTE terá direito a atualização de versão de todos os softwares contratados.

5.5. O serviço deverá ser prestado no idioma português.

5.6. A garantia será prestada com vistas a manter os equipamentos fornecidos em perfeitas condições de uso, sem qualquer ônus ou custo adicional para o Contratante.

5.7. A garantia abrange a realização da manutenção corretiva dos bens pela própria Contratada, ou, se for o caso, por meio de assistência técnica autorizada, de acordo com as normas técnicas específicas.

5.8. Entende-se por manutenção corretiva aquela destinada a corrigir os defeitos apresentados pelos bens, compreendendo a substituição de peças, a realização de ajustes, reparos e correções necessárias.

5.9. As peças que apresentarem vício ou defeito no período de vigência da garantia deverão ser substituídas por outras novas, de primeiro uso, e originais, que apresentem padrões de qualidade e desempenho iguais ou superiores aos das peças utilizadas na fabricação do equipamento.

5.10. Uma vez notificada, a Contratada realizará a reparação ou substituição dos bens que apresentarem vício ou defeito no prazo de até 24 (vinte e quatro) horas, contados a partir da data da notificação e/ou de retirada do equipamento das dependências da Administração pela Contratada ou pela assistência técnica autorizada.

5.11. O prazo indicado no subitem anterior, durante seu transcurso, poderá ser prorrogado uma única vez, por igual período, mediante solicitação escrita e justificada da Contratada, aceita pelo Contratante.

5.12. Na hipótese do subitem acima, a Contratada deverá disponibilizar equipamento equivalente, de especificação igual ou superior ao anteriormente fornecido, para utilização em caráter provisório pelo Contratante, de modo a garantir a continuidade dos trabalhos administrativos durante a execução dos reparos.

5.13. Decorrido o prazo para reparos e substituições sem o atendimento da solicitação do Contratante ou a apresentação de justificativas pela Contratada, fica o Contratante autorizado a contratar empresa diversa para executar os reparos, ajustes ou a substituição do bem ou de seus componentes, bem como a exigir da Contratada o reembolso pelos custos respectivos, sem que tal fato acarrete a perda da garantia dos equipamentos.

5.14. O custo referente ao transporte dos equipamentos cobertos pela garantia será de responsabilidade da Contratada.

5.15. A garantia legal ou contratual do objeto tem prazo de vigência próprio e desvinculado daquele fixado no contrato, permitindo eventual aplicação de penalidades em caso de descumprimento de alguma de suas condições, mesmo depois de expirada a vigência contratual.

6. PRAZOS E CONDIÇÕES DE ENTREGA E RECEBIMENTO

6.1. O prazo para entrega e instalação da solução deverá ocorrer em até 30 (trinta) dias consecutivos a partir do recebimento, pela CONTRATADA, da Nota de Empenho;

6.2. Entende-se por fornecimento dos produtos como a entrega efetiva de

todos os bens relacionados, conforme requisitos presentes no Termo de Referência, e sob requisição de quantitativos pelo CONTRATANTE, nas dependências deste Arquivo Nacional;

6.3. A execução dos serviços técnicos especializados on-site de instalação, configuração e customização das soluções adquiridas deverão ser executados a par r da entrega da solução pela CONTRATADA posterior à assinatura do contrato e posterior à entrega dos produtos;

6.4. Entende-se que tais serviços deverão contemplar a instalação de todas as licenças nos respec vos locais demandados pelo CONTRATANTE, configuração, testes, treinamento e entrega de documentação, prestados nas dependências do CONTRATANTE visando colocar os produtos (so ware e/ou hardware) em operação, devidamente instalados e configurados e com transferência de conhecimentos para a Equipe Técnica do AN;

6.5. Todo o processo de configuração e implantação da solução deverá ser feito por técnicos especializados da CONTRATADA cer ficados nas soluções propostas e será acompanhado e supervisionado pela área técnica;

6.6. A solução deverá ser fornecida com todos os recursos, componentes necessários para seu correto e adequado funcionamento, incluindo licenciamento do Sistema Operacional dos servidores e de banco de dados u lizado pela solução.

6.7. Após a entrega, a instalação e a configuração de todos os produtos pela CONTRATADA, a equipe técnica da CONTRATADA procederá os testes de funcionamento emi ndo o Termo de Recebimento Provisório em até 10 (dez) dias úteis;

6.8. O Gestor do Contrato emi rá o Termo de Recebimento Definitivo após a emissão de Termo de Recebimento provisório, para que, a par r deste momento, seja prestado os serviços de GARANTIA (manutenção e suporte técnico) estabelecidos no neste Termo de Referência;

6.9. Todo o fornecimento deve estar de acordo com os critérios estabelecidos nos itens deste Termo de Referência e em seus respectivos Anexos;

6.10. A entrega da solução e prestação de serviços deverão ser executadas, preferencialmente, de segunda a sexta-feira, em horário comercial;

6.11. Nos casos excepcionais, em que se faça necessária à interferência em ambientes de Produção, os serviços deverão ser executados em outros horários fora do es pulado acima, os quais deverão ser previamente agendados, com uma relação nominal dos profissionais da CONTRATADA que serão escalados, contendo identificação e os respectivos horários de trabalho;

6.12. O transporte dos componentes da solução até os locais de instalação deverá ser realizado pela CONTRATADA (inclusive os procedimentos de seguro, quando couber).

7. ENQUADRAMENTO DO OBJETO COMO COMUM

7.1. Os bens a serem adquiridos enquadram-se na classificação de bens comuns, nos termos da Lei n° 10.520, de 2002.

7.2. Os bens considerados comuns são aqueles cujos padrões de desempenho e qualidade possam ser objetivamente definidos pelo ato convocatório, por meio de especificações usuais do mercado, independentemente de sua complexidade.

7.3. As soluções de software Antivírus e AntiSpam são considerados comuns pois suas características são definidas de forma objetiva e amplamente praticadas pelo mercado especializado.

8. VALOR ESTIMADO DA CONTRATAÇÃO (REFERENCIAL)

Grupo	Item	Descrição do Item (Objeto)	Quantidade	Unidade de Medida	Valor (R$)	
					Unitário	Total
I	1	Solução corporativa de Antivírus para estações de trabalho com gerência em nuvem.	650	Unidade	260,00	69.000,00
	2	Solução corporativa de Antivírus para Servidores físicos e Virtuais com gerência em nuvem.	40	Unidade	525,00	21.000,00
	3	Solução de segurança anti-spam e e-mail gateway	750	Unidade	116,86	87.648,11
	Valor Total					**277.648,11**

Obs: *O detalhamento da pesquisa de preços encontra-se no inserido nos Documentos SEI nº 0043571 e 0043573, que farão parte do processo licitatório.*

9. ALINHAMENTO ESTRATÉGICO

9.1. Para subsidiar a execução de suas atribuições de maneira cada vez mais democrática, combinando a contínua melhoria do atendimento à necessidade do órgão, sem os quais não seria possível atender às demandas, estratégias, garantir a governança e a efetividade da gestão de TI e melhorar continuamente a prestação de serviços e qualidade das informações fornecidas à sociedade. Além disso, os resultados esperados com a pretensa aquisição, contribuirão para os desafios estratégicos da COTIN/AN para os próximos anos.

10. OBRIGAÇÕES DA CONTRATADA

10.1. Receber os bens adjudicados nas condições integrais dos itens licitados, observados os dispositivos legais quanto ao RECEBIMENTO PROVISÓRIO e DEFINITIVO, além de exigir e regular o cumprimento das obrigações complementares, em especial aquelas relativas à garantia técnica, suporte e treinamento;

10.2. Promover o acompanhamento e a fiscalização da execução do objeto do presente Termo de Referência, sob o aspecto quantitativo e qualitativo, anotando em registro próprio as falhas detectadas;

10.3. Comunicar prontamente à CONTRATADA qualquer anormalidade na execução do objeto, podendo recusar o recebimento caso não esteja de acordo com as especificações e condições estabelecidas no presente Termo de Referência;

10.4. Fornecer à CONTRATADA todo tipo de informação interna essencial à realização dos fornecimentos e dos serviços;

10.5. Permitir o acesso dos funcionários da CONTRATADA, desde que devidamente identificados, às suas dependências para a devida realização dos serviços e fornecimento dos bens contratados;

10.6. Conferir toda a documentação técnica gerada e apresentada durante a execução dos serviços, efetuando o seu atesto quando a mesma estiver em conformidade com os padrões de informação e qualidade exigidos.

10.7. Homologar os serviços prestados, quando os mesmos estiverem de acordo com o especificado no Termo de Referência;

10.8. Rejeitar os objetos entregues e serviços realizados fora do estabelecido e que estejam em desacordo com o Contrato.

10.9. Proceder às advertências, multas e demais comunicações legais pelo descumprimento dos termos deste instrumento.

10.10. Efetuar o pagamento à CONTRATADA, de acordo com o estabelecido no Edital e seus Anexos.

10.11. Sustar o pagamento de faturas no caso de inobservância, pela Contratada, de condições contratuais;

10.12. Emitir Termo de Recebimento Provisório e Termo de Recebimento Definitivo.

11. OBRIGAÇÕES DA CONTRATANTE

11.1. Atender a todas as condições descritas no presente Termo de Referência e respectivo Contrato;

11.2. Manter as condições de habilitação e qualificação exigidas durante toda a vigência do Contrato;

11.3. Facilitar o pleno exercício das funções da fiscalização. O não atendimento das solicitações feitas pela fiscalização será considerado motivo para aplicação das sanções contratuais. O exercício das funções da fiscalização não desobriga a contratada de sua própria responsabilidade quanto à adequada execução do objeto contratado;

11.4. Entregar os bens e prestar os serviços de acordo com os requisitos de quantidades, especificações técnicas, manuais de operação (quando couber).

11.5. Entregar os bens e prestar os serviços, impreterivelmente, no prazo previsto e local designado, conforme especificações constantes da proposta e do Edital e seus Anexos.

11.6. Não divulgar informações, conceder entrevistas ou qualquer tipo de divulgação na mídia geral sobre projetos do CONTRATANTE sem alinhamento prévio com a diretoria/coordenação a que se reporta. Não utilizar a marca do CONTRATANTE sem alinhamento prévio e autorização deste.

11.7. Prestar garantia técnica na forma e condições estabelecidas.

11.8. Indicar, formalmente, observado o art. 68, da Lei n.º 8.666, de 1993, Preposto para acompanhar a execução dos serviços e responder perante a CONTRATANTE.

11.9. Arcar com todos os encargos diretos e indiretos que incidir sobre a comercialização, instalação, garantia técnica integral, suporte e treinamentos contratados em face da venda dos produtos licitados, inclusive sob eventuais substituições e reposições.

11.10. Assumir a responsabilidade por todas as providências e obrigações estabelecidas na legislação específica de acidentes do trabalho, quando forem vítimas os seus profissionais no desempenho dos serviços objeto deste instrumento ou em conexão com eles, ainda que acontecido nas dependências do CONTRATANTE.

11.11. Pagar os tributos, taxas e encargos de qualquer natureza de sua responsabilidade em decorrência do Contrato;

11.12. Não ceder ou transferir, total ou parcialmente, parte alguma do contrato. A fusão, cisão ou incorporação só serão admitidas com o consentimento prévio e por escrito do CONTRATANTE;

11.13. Toda informação referente às Áreas de TI de cada Órgão que a Contratada, seus Prepostos e Técnicos vierem a tomar conhecimento por necessidade de execução dos serviços contratados, não poderá, sob hipótese nenhuma, ser divulgada a terceiros.

11.14. Assumir todos os custos por eventuais deslocamentos da equipe do CONTRATANTE que porventura se façam necessários para fins de atualização tecnológica, reforço de capacitação, conhecer ambientes laborais com solução similar implantada, laboratórios, fábricas, ou seja, todo e qualquer evento que tenha por finalidade agregar conhecimento e potencializar a solução adquirida por parte da equipe do CONTRATANTE.

11.15. Não deixar de executar qualquer atividade necessária ao perfeito fornecimento do objeto, sob qualquer alegação, mesmo com pretexto de não ter sido executado anteriormente qualquer tipo de procedimento;

11.16. Manter central de suporte técnico, indicando o número de telefone desta ou endereço eletrônico para abertura de chamados.

11.17. Deverá a CONTRATADA possuir profissionais devidamente habilitados e qualificados à prestação de assistência técnica, durante todo o período garantia de software.

11.18. Providenciar a substituição imediata dos profissionais alocados ao serviço, que eventualmente não atendam aos requisitos deste Termo de Referência ou por solicitação do CONTRATANTE, devidamente justificada;

11.19. Responsabilizar-se por danos causados ao patrimônio do CONTRATANTE e suas unidades, ou de terceiros, ocasionados por seus empregados, em virtude de dolo ou culpa, durante a execução do objeto contratado;

11.20. Responsabilizar-se por quaisquer acidentes de que possam ser vítimas seus empregados e prepostos, quando nas dependências do CONTRATANTE e respectivas unidades, devendo adotar as providências que, a respeito, exigir a legislação em vigor;

12. CRITÉRIOS DE HABILITAÇÃO TÉCNICA

12.1. 13.1. Será requerida das empresas licitantes, para fins de habilitação, a comprovação de aptidão para a prestação dos serviços em características e quantidades compatíveis com o objeto desta licitação, mediante a apresentação de:

12.1.1. atestado(s) de capacidade técnica, emitido(s) por pessoa(s) jurídica(s) de direito público ou privado, que comprove(m) ter fornecido ou estar fornecendo softwares compatíveis em características, prazos e em quantidade de ao menos 40% (quarenta por cento) do quantitativo de cada item do objeto da licitação;

12.1.2. declaração informando se a licitante é a fabricante, revendedora ou

distribuidora autorizada do fabricante, ou ainda, revendedora autorizada de distribuidor autorizado pelo fabricante dos produtos. Caso a licitante não possua uma das qualificações exigidas anteriormente, deverá ser apresentada declaração do próprio licitante de que a aquisição dos softwares, objeto desse edital, será realizada através de um canal do fabricante, para softwares especificados pelo fabricante para uso no Brasil.

12.2. Tais declarações deverão ser emitidas em papel timbrado, com assinatura, identificação e telefone do emitente.

12.3. Admite-se mais de um atestado com vistas a comprovar o atendimento a todos os requisitos de capacidade técnica que asseguram a similaridade do objeto.

12.4. A licitante disponibilizará todas as informações necessárias à comprovação da legitimidade do(s) atestado(s).

12.5. A comprovação de capacidade deverá ser realizada por meio de atestado ou conjunto de atestados que totalizados atendam aos critérios e volumes mínimos exigidos.

12.6. No caso de atestados emitidos por empresa da iniciativa privada, não serão considerados válidos aqueles emitidos por empresas pertencentes ao mesmo grupo empresarial da licitante. Serão consideradas como pertencentes ao mesmo grupo empresarial as empresas controladas ou controladoras da empresa licitante, e ainda as que tenham pelo menos uma pessoa física ou jurídica como sócia em comum.

12.7. O CONTRATANTE reserva-se o direito de realizar diligências, a qualquer momento, com o objetivo de verificar se o(s) atestado(s) e demais documentos são adequados e atendem às exigências contidas neste Termo de Referência, podendo exigir apresentação de documentação complementar referente à prestação de serviços relativos aos atestados apresentados.

12.8. Caso a licitante não comprove as exigências do Edital por meio das documentações requeridas, será desclassificada.

12.9. O pregoeiro examinará a proposta classificada em primeiro lugar quanto à compatibilidade do preço em relação ao estimado para a contratação, de acordo com as exigências do Edital.

13. SUBCONTRATAÇÃO

13.1. Não será admitida a subcontratação do objeto licitatório

14. ALTERAÇÃO SUBJETIVA

14.1. É admissível a fusão, cisão ou incorporação da CONTRATADA com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da Administração à continuidade do contrato.

15. MODELO DE EXECUÇÃO E GESTÃO CONTRATUAL

15.1. PAPÉIS E RESPONSABILIDADES

15.1.1. Gestor do Contrato: coordenar e comandar o processo de gestão e fiscalização da execução contratual, nos termos da subseção III da Seção III IN

01/2019, da Secretaria de Governo Digital do Ministério da Economia.

15.1.2. Fiscal Técnico: fiscalizar tecnicamente o contrato, nos termos da subseção III da Secão III IN 01/2019, da Secretaria de Governo Digital do Ministério da Economia.

15.1.3. Fiscal Requisitante: fiscalizar o contrato do ponto de vista funcional da Solução de Tecnologia da Informação, nos termos da subseção III da Secão III IN 01/2019, da Secretaria de Governo Digital do Ministério da Economia.

15.1.4. Fiscal Administrativo: fiscalizar o contrato quanto aos aspectos administrativos, nos termos da subseção III da Secão III IN 01/2019, da Secretaria de Governo Digital do Ministério da Economia.

15.1.5. Preposto da CONTRATADA: acompanhar a execução do contrato e atuar como interlocutor principal junto ao CONTRATANTE, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual.

15.1.6. Analistas e técnicos da CONTRATADA: realizar a entrega dos bens e executar os serviços relacionados ao objeto.

15.2. FISCALIZAÇÃO

15.2.1. O gestor do contrato e os fiscais representarão o CONTRATANTE e terão as atribuições delegadas em ato específico.

15.2.2. Agir e decidir em nome do CONTRATANTE, inclusive, para rejeitar o objeto contratado, quando em desacordo com as especificações exigidas.

15.2.3. Certificar as faturas correspondentes e encaminhá-las à Área Administrativa do órgão, após constatar o fiel cumprimento das obrigações contratuais.

15.2.4. Exigir da EMPRESA o cumprimento rigoroso das obrigações assumidas.

15.2.5. Emitir os Termos de Recebimento Provisório e Definitivo, nos termos do artigo 33 da IN nº 01/2019 da Secretaria de Governo Digital do Ministério da Economia.

15.2.6. A fiscalização de que trata este item não exclui nem reduz a responsabilidade da CONTRATADA, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas ou vícios redibitórios, e, na ocorrência desta, não implica em corresponsabilidade da Administração ou de seus agentes e prepostos, de conformidade com o art. 70 da Lei nº 8.666, de 1993.

15.2.7. No exercício de suas atribuições fica assegurado à FISCALIZAÇÃO, sem restrições de qualquer natureza, o direito de acesso a todos os elementos de informações relacionados com o objeto do Contrato.

15.2.8. O representante da Administração anotará em registro próprio todas as ocorrências relacionadas com a execução do contrato, indicando dia, mês e ano, bem como o nome dos funcionários eventualmente envolvidos, determinando o que for necessário à regularização das falhas ou defeitos observados e encaminhando os apontamentos à autoridade competente para as providências cabíveis.

15.3. METODOLOGIA DE AVALIAÇÃO DA QUALIDADE E ACEITE DOS BENS FORNECIDOS

15.3.1. Todo o trabalho realizado pela CONTRATADA estará sujeito à avaliação

técnica, sendo homologado quando estiver de acordo com o padrão de qualidade exigido pelo órgão e de acordo com os prazos definidos;

15.3.2. A documentação técnica gerada deverá seguir o padrão acordado entre o CONTRATANTE e a CONTRATADA, sendo devidamente verificada por responsável técnico e atestada pelo Fiscal do Contrato;

15.3.3. A solução será considerada aceita quando da instalação e perfeito funcionamento da solução e entrega de todas as licenças que a compõem, incluindo licenças de sistemas operacionais e bancos de dados, em nome da CONTRATANTE, assim como entrega da respectiva documentação técnica, que inclui o respectivo projeto de implantação e tabela de licenças de software.

15.3.4. Além dos prazos de entrega, serão consideradas como critérios de aceite as características técnicas das soluções.

15.3.5. O objeto deste Termo de Referência será dado como recebido de acordo com os artigos 73 a 76 da Lei 8.666/93;

15.3.6. Para aceite do recebimento e posterior encaminhamento ao pagamento, deverão ser apresentados os seguintes documentos:

a) *Termo de Entrega e Tabela de Licenças*

b) *Termo de Aceite de Serviços*

15.3.7. Independentemente da aceitação no recebimento, a CONTRATADA

15.3.8. deverá garantir a qualidade do serviço e produtos fornecidos pelo prazo estabelecido nas especificações e nas condições constantes deste Termo de Referência, obrigando-se a corrigir aquele que apresentar erro ou defeito, no prazo estabelecido pelo CONTRATANTE.

15.3.9. São critérios de mensuração dos serviços para efeito de pagamento:

CRITÉRIOS DE MENSURAÇÃO		
Evento	**Documentos**	**Valor**
• Solução entregue, com garantia emitida (36 meses) Serviços de instalação, para Antivírus e (12 meses) para anti-spam e e-mail gateway • Repasse de conhecimento executado (100%)	• Termo de Entrega e Tabela • Termo de Aceite de constantes da Proposta Serviços	• Valor total referente aos Serviços de instalação, de Licenças produtos e serviços, configuração/parametrização conforme os valores executados (100%) • Comercial/Contrato

15.4. SANÇÕES ADMINISTRATIVAS (PENALIDADES)

15.4.1. Comete infração administrativa nos termos da Lei nº 8.666, de 1993 e da Lei nº 10.520, de 2002, a CONTRATADA que:

a) inexecutar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;

b) ensejar o retardamento da execução do objeto;

c) fraudar na execução do contrato;

d) comportar-se de modo inidôneo;

e) cometer fraude fiscal;

f) não mantiver a proposta.

15.4.2. A CONTRATADA que cometer qualquer das infrações discriminadas no subitem acima ficará sujeita, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

a) advertência por faltas leves, assim entendidas aquelas que não acarretem prejuízos significativos para a CONTRATANTE;

b) multa moratória de 0,1% (um décimo por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 20 (vinte) dias;

c) multa compensatória de 5% (cinco por cento) sobre o valor total do contrato, no caso de inexecução total do objeto;

d) em caso de inexecução parcial, a multa compensatória, no mesmo percentual do subitem acima, será aplicada de forma proporcional à obrigação inadimplida;

e) suspensão de licitar e impedimento de contratar com o órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente, pelo prazo de até dois anos;

f) impedimento de licitar e contratar com a União com o consequente descredenciamento no SICAF pelo prazo de até cinco anos;

g) declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a CONTRATADA ressarcir a CONTRATANTE pelos prejuízos causados;

15.4.3. Também ficam sujeitas às penalidades do art. 87, III e IV da Lei nº 8.666, de 1993, as empresas ou profissionais que:

a) tenham sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no recolhimento de quaisquer tributos;

b) tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;

c) demonstrem não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

15.4.4. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à CONTRATADA, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente a Lei nº 9.784, de 1999.

15.4.5. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

15.4.6. As penalidades serão obrigatoriamente registradas no SICAF.

15.5. PAGAMENTO

15.5.1. O pagamento será efetuado, mediante apresentação de Nota Fiscal devidamente atestada pelo setor competente, após conclusão e aceite dos serviços

por meio da emissão do termo de recebimento definitivo.

15.5.2. O pagamento será realizado em parcela única no prazo máximo de até 30 (trinta) dias, contados a partir da data final do período de adimplemento a que se referir, através de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo contratado.

15.5.3. Os pagamentos decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 24 da Lei 8.666, de 1993, deverão ser efetuados no prazo de até 5 (cinco) dias úteis, contados da data da apresentação da Nota Fiscal, nos termos do art. 5º, § 3º, da Lei nº 8.666, de 1993.

15.5.4. Havendo erro na fatura ou circunstâncias que impeçam a liquidação da despesa, aquela será devolvida e o pagamento ficará pendente até que a empresa providencie as medidas saneadoras do problema. Nesta hipótese, o prazo para o pagamento iniciar-se-á após a regularização da situação e/ou reapresentação da fatura, não acarretando qualquer ônus para o Arquivo Nacional.

15.6. DISPONIBILIDADE ORÇAMENTÁRIA

15.6.1. A despesa decorrente da contratação deverá correr a conta do Programa de Trabalho consignado de cada órgão participante da ata de registro de preços na respectiva quantidade de cada item.

15.7. REAJUSTE

15.7.1. Os preços são fixos e irreajustáveis no prazo de um ano contado da data limite para a apresentação das propostas.

15.8. VIGÊNCIA DA CONTRATAÇÃO

15.8.1. O prazo de vigência da contratação para os serviços relativos ao **Grupo I (Itens 1 e 2) vigorará por 36 (trinta e seis) meses** e para o **Item 3 será de 12 (doze) meses,** contados a partir do primeiro dia útil subseqüente à data da assinatura do contrato.contados a partir da data de sua assinatura, com relação manutenção durante o período de garantia “on site”.

15.8.2. O prazo de vigência contratual compreende o período previsto para a entrega, Implantação e configuração da solução, até o aceite definitivo, sem prejuízo dos prazos de garantia estabelecidos na contratação.

16. QUALIFICAÇÕES

16.1. A qualificação dos proponentes deve ser realizada de acordo com o estabelecido no art. 27 da Lei nº 8.666, de 21 de junho de 1993.

17. MODALIDADE/TIPO DE LICITAÇÃO

17.1. Este planejamento foi elaborado de acordo com o Ordenamento Jurídico Nacional que regulamenta o processo de aquisições para a Administração Publica, ou seja: Lei no 8.666, de 21 de junho de 1993; Lei no 10.520, de 17 de julho de 2002; Decreto no 5.450, de 31 de maio de 2005; e Instrução Normativa SLTI/MP no 04, de 12 de novembro de 2014.

17.2. Destacando também a observação da legislação específica exarada no Decreto no 7.174, de 12 de maio de 2010, que disciplina as condições especiais para

a aquisição de bens e contratação de serviços de TIC para os órgãos e entidades sob controle da União.

17.3. Em se tratando de um Registro de Preços, o Decreto no 7.892, de 2013, determina a adoção das modalidades Concorrência Publica ou Pregão, sendo que para o ultimo e obrigatório o uso do tipo menor preço.

17.4. Deste modo, o presente documento contem os elementos básicos e essenciais determinados pela legislação, descritos de forma a subsidiar os interessados em participarem do certame licitatório na preparação da documentação e na elaboração da proposta.

17.5. Os bens que constituem o Objeto deste Planejamento da Contratação enquadram-se no conceito de bem comum, nos termos do Decreto no 7.174/2010, onde os requisitos técnicos são suficientes para determinar o conjunto da solução escolhida e o bem e fornecido comercialmente por mais de uma empresa no mercado.

17.6. Assim, entende-se que a modalidade de licitação devera ser PREGÃO, a ser realizada na forma ELETRÔNICA, do tipo menor preço, com vistas a obter a melhor proposta para a Administração Publica.

17.7. Em virtude de acudir o maior numero de interessados em participar da licitação sem prejudicar o ganho de aquisição em escala, razão motivadora da realização das compras conjuntas, optou-se por pela divisão em GRUPO, sempre em respeito a mais ampla competição e conforme previsto no art. 23, §§ 1o e 2o, da Lei no 8.666/93, Sumula no 247 do TCU e Acórdão do TCU no 786/2006 e 116/2006, todos do Plenário do TCU.

18. CRITÉRIOS TÉCNICOS DE JULGAMENTO

18.0.1. ORGANIZAÇÃO DA PROPOSTA

18.0.1.1. As propostas deverão ser apresentadas de forma clara e objetiva, em conformidade com o instrumento convocatório, e conterão todos os elementos que influenciem no valor final da contratação, dentre os quais:

a) Preços unitários, valor total e global da proposta, conforme disposto no instrumento convocatório.

b) O prazo de **validade da proposta** comercial não poderá ser inferior a **60 (sessenta) dias** a contar da data de abertura do certame licitatório.

18.0.1.2. A seleção do fornecedor dar-se-á por meio de licitação, na modalidade Pregão, na forma eletrônica, tipo **menor preço por lote.**

18.0.1.3. Deverá ser numerada sequencialmente a fim de permitir maior agilidade no seu manuseio durante a conferência e o exame correspondente das informações e documentos.

18.0.1.4. A proposta de preço deverá ser assinado por proprietário, sócio ou preposto da licitante, com poderes para tal, instituídos em instrumento de procuração pública ou particular; tudo devidamente comprovado com a apresentação dos originais ou cópias autenticadas, inclusive do documento de identidade do outorgante e do outorgado, se for o caso.

18.0.1.5. Não será permitida a diferenciação do conteúdo da proposta apresentada, em relação a preço, pagamento, prazo ou a qualquer outra condição constante neste Termo de Referência e resultado do Pregão Eletrônico, sob pena de

desclassificação da licitante.

18.0.1.6. A proposta deverá conter o número de telefone e fax, no Rio de Janeiro/RJ ou número 0800 e o e-mail (correio eletrônico), onde poderão ser efetuados os contatos necessários durante o período de vigência do contrato.

18.0.1.7. É vedada qualquer indexação de preços por índices gerais, setoriais ou que reflitam a variação de custos.

18.0.1.8. As propostas apresentadas deverão ser analisadas e julgadas de acordo com o disposto nas normas legais vigentes, e ainda em consonância ao estabelecido no instrumento convocatório.

18.0.1.9. Serão desclassificadas as propostas que:

a) Contenham vícios ou ilegalidades;

b) Não apresentem as especificações técnicas exigidas neste Termo de Referencia.

19. SIGILO E INVIOLABILIDADE

19.1. A contratada deverá garantir o sigilo e a inviolabilidade das informações a que eventualmente possa ter acesso durante os procedimentos de assistência técnica.

20. ANEXOS

20.1. ANEXO I - Modelo de Termo de Recebimento Provisório (SEI nº 0005993)

20.2. ANEXO II - Modelo de Termo de Recebimento Definitivo (SEI nº 0005994)

20.3. ANEXO III - Ordem de Serviço/Recebimento de Bens (SEI nº 0005996).

20.4. ANEXO IV - Termo de Compromisso de Manutenção de Sigilo (SEI nº 0005997).

Integrante Requisitante	Integrante Técnico	Integrante Administrativo
Bruno de Freitas Tavares da Silva Siape nº 2003580	Julio Cesar Cavadas Fernandes Siape nº 6222313	Patrick Jubilado Xerém Siape nº 2747089

O presente documento segue assinado pelo servidor Elaborador, pela Equipe de Planejamento (Integrante Demandante, Integrante Técnico e Integrante Administrativo e pela autoridade máxima da Área de TIC e aprovado pela autoridade competente, de acordo com o §6º do artigo 12, subseção III da Secão I da IN 01/2019, da Secretaria de Governo Digital do Ministério da Economia.

Documento assinado eletronicamente por **Maximiliano Martins de Faria**, **Coordenador de Tecnologia da Informação**, em 17/11/2020, às 12:36, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Bruno de Freitas Tavares da Silva**, **Técnico em Tecnologia da Informação**, em 17/11/2020, às 13:28,

conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Julio Cesar Cavadas Fernandes**, **Operador de Computador**, em 17/11/2020, às 16:32, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Leandro Esteves de Freitas**, **Coordenador-Geral de Administração**, em 18/11/2020, às 15:15, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Patrick Jubilado Xerém**, **Agente administrativo**, em 22/11/2020, às 08:50, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.arquivonacional.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0062672** e o código CRC **79D06DE6**.

Modelo elaborado pela Secretaria de Governo Digital - Versão Publicada em 30/01/2020 19h40