PREGÃO ELETRÔNICO Nº 057/2026

ENTIDADE: Município de Piraí **ESTADO**: Rio de Janeiro

ÓRGÃO: Secretaria Municipal de Ciência e Tecnologia

PROCESSO ADMINISTRATIVO Nº. PIR-020210/000248/2026

AGENTE DE CONTRATAÇÃO/PREGOEIRO: Alexandre Gaudêncio Machado

DESIGNAÇÃO DO AGENTE DE CONTRATAÇÃO/PREGOEIRO: Portaria nº 499/2025

PLATAFORMA DE REALIZAÇÃO:

ENDEREÇO ELETRONICO: www.novobbmnet.com.br

RECEBIMENTO DAS PROPOSTAS ATÉ: 02/09/2026 – Horas 08:00:00

ABERTURA E ANÁLISE DAS PROPOSTAS: 02/09/2026 – Horas 09:00:00

INÍCIO DA ETAPA DE LANCES: 02/09/2026 – Horas 09:05:00

Obs: (podendo apresentar um delay mínimo de segundos, ou milésimos de segundos, entre o início e o término dos lances)

REFERÊNCIA DE TEMPO: Para todas as referências de tempo será observado o horário de Brasília/DF e, dessa forma, serão registradas no sistema eletrônico e na documentação relativa ao certame.

1. PREÂMBULO

1.1. O MUNICÍPIO DE PIRAÍ/RJ, CNPJ nº 29.141.322/0001-32, por intermédio da Secretaria Municipal de ADMINISTRAÇÃO, sito na Rua Dr. Luiz Antônio Garcia da Silveira, nº 16, Centro, em Piraí, Estado do Rio de Janeiro, por meio do Pregoeiro, designados pela Portaria nº 499/2025, atendendo requisitos do Processo Administrativo nº PIR-020210/000248/2026, torna público que, será realizada licitação, com participação AMPLA, na modalidade PREGÃO, na forma ELETRÔNICA, no modo de disputa ABERTO, critério de julgamento MENOR PREÇO GLOBAL, nos termos da Lei Federal 14.133/21 – Lei de licitações e contratos administrativos, com aplicação subsidiária, da Instrução Normativa SEGES/ME nº 73/22 – Licitação eletrônica para contratação de bens, serviços e obras, da Lei Complementar Federal nº 123/06 – Estatuto Nacional da Microempresa e da Empresa de Pequeno Porte, e demais normas que compõem a legislação aplicável à licitações e contratações públicas, observadas as alterações posteriores introduzidas nos referidos diplomas legais, e disposto no presente Edital;

Prefeitura Municipal de Piraí APROVADO Assessoria Jurídica

Prefeitura Municipal de Piraí Secretaria Municipal Administração Estado do Rio

1.2. A sessão pública de processamento do Pregão Eletrônico será realizada no endereço eletrônico **www.novobbmnet.com.br**, no dia e hora indicados neste Edital e conduzida pelo Pregoeiro com o auxílio de sua equipe de apoio, todos designados nos autos do processo em epígrafe;

1.3. O Aviso de Licitação se encontra disponível no endereço eletrônico, http://www.pirai.rj.gov.br/transparencia/contratoselicitações/.

1.4. O procedimento será divulgado no www.novobbmnet.com.br e no Portal Nacional de Contratações Públicas – PNCP.

1.5. O fornecedor é o responsável por qualquer transação efetuada diretamente ou por seu representante no Sistema, não cabendo ao provedor do Sistema ou ao órgão entidade promotor do procedimento a responsabilidade por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros não autorizados

2. DO OBJETO

2.1. Objeto deste pregão eletrônico é a Aquisição de solução integrada (Harwdware/Software) de Firewall de Próxima Geração Tipo 1, conforme especificações constantes no Anexo I, Termo de Referência, deste edital.

2.2. No caso de divergência entre a especificação contida neste edital e no Sistema www.novobbmnet.com.br, prevalecerá a descrita neste edital.

3. DO PREÇO MÁXIMO ESTIMADO PARA PROPOSTA

3.1. O preço máximo que a Administração se propõe a pagar no objeto deste edital é de **R$ 223.000,00** (duzentos e vinte e três mil reais) acima do qual, as propostas serão desclassificadas, nos termos do Artigo 59, Inciso III, da Lei Federal nº 14.133/2021 e suas alterações.

3.2. O preço máximo unitário admitido pela Administração encontra-se fixado no Termo de Referência, Anexo I, deste Edital.

4. DOS RECURSOS ORÇAMENTÁRIOS

As despesas com a execução do objeto deste Pregão correrá pelas dotações orçamentárias: 11101957200142213339040001500000 e 11101957200142213449052001500000

5. DAS CONDIÇÕES DE PARTICIPAÇÃO

5.1. Somente poderão participar deste certame as empresas que estejam legalmente estabelecidas e explorem ramo de atividade compatível com o objeto desta licitação, devendo tal fato ser oportunamente comprovado mediante exame dos atos constitutivos da empresa;

Prefeitura Municipal de Piraí – APROVADO – Assessoria Jurídica

Prefeitura Municipal de Piraí – Secretaria Municipal Administração – Estado do Rio

5.2. Disponham de chave de identificação e senha pessoal, obtidas junto ao provedor do sistema, bem como informar-se a respeito do seu funcionamento e regulamento e receber instruções dos gestores do sistema www.novobbmnet.com.br para sua correta utilização;

5.3. Atendam às condições exigidas neste Edital e em seus Anexos;

5.4. Poderão participar as empresas que cumpram os requisitos legais para efeito de qualificação como Microempresa ou Empresa de Pequeno Porte ou Equiparadas, e que não se enquadrem em nenhuma das hipóteses elencadas no § 4º do art. 3º da Lei Complementar nº 123/2006, estando aptas a usufruir dos direitos de que tratam os artigos 42 a 49 da mencionada Lei, não havendo fatos supervenientes impeditivos da participação no presente certame.

5.5. As microempresas (ME), empresas de pequeno porte (EPP) e equiparadas que desejarem participar do procedimento licitatório deverão observar a condição prevista no parágrafo 1º, inciso I, e nos parágrafos 2º e 3º do artigo 4º da Lei Federal 14.133/21.

5.5.1. A participação e a concessão dos benefícios legais serão limitados às microempresas e às empresas de pequeno porte que, no ano calendário de realização da licitação, ainda não tenham celebrado contratos com a Administração Pública e iniciativa privada cujos valores somados extrapolem a receita bruta máxima admitida para fins de enquadramento como empresa de pequeno porte, devendo a licitante apresentar declaração de observância desse limite na licitação, de acordo com o parágrafo 2º do artigo 4º da Lei Federal 14.133/21 e formato similar da Instrução Normativa SEGES ME 05/2017 – Anexo VII-E.

5.6. Diante das hipóteses suscitadas no item 5.5, caso a licitante ME EPP optante do Simples Nacional venha ser adjudicada e adquira o status de desenquadramento, deverá providenciar comunicação junto à Secretaria da Receita Federal do Brasil-RFB, até o último dia útil do mês subsequente ao da ocorrência da situação de vedação (celebração do Contrato ou instrumento equivalente), apresentando ao Município de Piraí, no prazo de 90 (noventa) dias contados da assinatura do termo contratual, comprovação da efetivação das providências para a exclusão obrigatória prevista nos artigos 30 e 31, incisos II, da Lei Complementar nº 123/2006;

5.7. Caso a licitante optante pelo SIMPLES NACIONAL não efetue, nesse caso, a comunicação no prazo assinalado acima, o próprio Município de Piraí, em obediência ao princípio da probidade administrativa, efetuará a comunicação à Secretaria da Receita Federal do Brasil-RFB, para que esta efetue a exclusão de ofício, conforme disposto no inciso I do artigo 29 da Lei Complementar nº 123, de 14 de dezembro de 2006 e alterações;

5.8. Será permitida a participação em consórcio, sujeita às seguintes regras:

5.8.1. As empresas consorciadas apresentarão instrumento público ou particular de compromisso de constituição de consórcio, subscrito por todas elas, indicando a empresa líder, que será responsável principal, pelos atos praticados pelo Consórcio, sem prejuízo da responsabilidade solidária;

5.8.2. Apresentarão, de forma conjunta, mas individualizada, documentação de habilitação prevista nos itens 14 a 18;

5.8.3. As empresas consorciadas não poderão participar da licitação isoladamente, nem por intermédio de mais de um consórcio;

5.8.4. As empresas consorciadas responderão solidariamente pelos atos praticados em consórcio, tanto na fase da licitação quanto na da execução do Contrato;

5.9. O consórcio vencedor, quando for o caso, ficará obrigado a promover a sua constituição e registro antes da celebração do Contrato.

6. DA VEDAÇÃO À PARTICIPAÇÃO NO CERTAME

6.1. Não poderão disputar esta licitação direta ou indiretamente:

6.1.1. aquele que não atenda às condições deste Edital e seu(s) anexo(s);

6.1.2. pessoa física ou jurídica que se encontre, ao tempo da licitação, impossibilitada de participar da licitação em decorrência de sanção que lhe foi imposta;

6.1.2.1. O impedimento de que trata o item anterior será também aplicado ao licitante que atue em substituição a outra pessoa, física ou jurídica, com o intuito de burlar a efetividade da sanção a ela aplicada, inclusive a sua controladora, controlada ou coligada, desde que devidamente comprovado o ilícito ou a utilização fraudulenta da personalidade jurídica do licitante;

6.2. Agente público de órgão ou entidade licitante ou contratante, devendo ser observadas as situações que possam configurar conflito de interesses no exercício ou após o exercício do cargo ou emprego, nos termos da legislação que disciplina a matéria;

6.3. Aquele que mantenha vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão, entidade contratante ou com agente público que desempenhe função na licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau;

6.4. Empresas controladoras, controladas ou coligadas, nos termos da Lei Federal nº 6.404/76, concorrendo entre si;

6.5. Pessoa física ou jurídica que, nos 5 (cinco) anos anteriores à divulgação do edital, tenha sido condenada judicialmente, com trânsito em julgado, por exploração de trabalho infantil, por submissão de trabalhadores a condições análogas às de escravo ou por contratação de adolescentes nos casos vedados pela legislação trabalhista;

6.6. Sociedades integrantes de um mesmo grupo econômico, assim entendidas aquelas que tenham diretores, sócios ou representantes legais comuns, ou que utilizem recursos materiais, tecnológicos ou humanos em comum;

7. DA APRESENTAÇÃO DAS PROPOSTAS E OUTROS DOCUMENTOS

7.1. As licitantes encaminharão, exclusivamente por meio do sistema eletrônico www.novobbmnet.com.br, suas respectivas propostas com a descrição do objeto e os preços ofertados, conforme o critério de julgamento adotado neste Edital, até a data e o horário estabelecidos para abertura da sessão pública, quando, então, encerrar-se-á automaticamente a etapa de envio dessa documentação;

7.2. A verificação da conformidade da proposta será feita exclusivamente na fase de julgamento, em relação à proposta mais bem classificada, na forma do § 1º do artigo 20 da Instrução Normativa SEGES nº 73/2022;

7.3. Além de outras informações demandadas pelo sistema eletrônico, deverão consignar que compreendem a descrição do(s) produto(s) ofertado(s), o(s) preço(s) unitário(s) e total(ais) do(s) item(ns) para o(s) qual(ais) pretende oferecer proposta, de acordo com o TERMO DE REFERÊNCIA – ANEXO I deste edital; que a proposta formulada está compatível com o edital e seus anexos; o prazo de fornecimento do objeto, contado do recebimento da solicitação da Secretaria Municipal Solicitante; o prazo de validade da proposta comercial;

7.4. Os licitantes não poderão oferecer proposta em quantitativo inferior ao máximo previsto no edital de licitação;

7.5. No cadastramento da proposta inicial, o licitante declarará, em campo próprio do sistema, que:

7.5.1. está ciente do inteiro teor do edital e seus anexos, e que concorda com suas condições, respondendo pela veracidade das informações prestadas, na forma da lei;

7.5.2. a proposta apresentada compreende a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal de 1988, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de sua entrega em definitivo;

7.5.3. cumpre plenamente os requisitos de habilitação e que sua proposta está em conformidade com as exigências desse Edital e do Termo de Referência;

7.5.4. cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas, conforme previsto no inciso IV do artigo 63 da Lei Federal nº 14.133/2021;

7.5.5. não emprega menores de 18 anos em trabalho noturno, perigoso ou insalubre, nem menores de dezesseis anos em qualquer trabalho, salvo na condição de aprendiz, a partir dos quatorze anos, nos termos do artigo 7°, XXXIII, da Constituição;

7.6. No caso de licitante enquadrada como microempresa, empresa de pequeno porte ou sociedade cooperativa deverá declarar, ainda, em campo próprio do sistema eletrônico, 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 artigos 42 a 49, observado o disposto nos §§ 1º ao 3º do art. 4º, da Lei nº 14.133/ 2021.

7.6.1. no item exclusivo para participação de microempresas e empresas de pequeno porte, a assinalação do campo "não" impedirá o prosseguimento no certame, para aquele item;

7.7. A falsidade da declaração de que trata os subitens 7.5 sujeitará o licitante às sanções previstas na Lei nº 14.133/2021, e neste Edital;

7.8. Os licitantes poderão retirar ou substituir a proposta(s) ou, na hipótese de a fase de habilitação anteceder as fases de apresentação de propostas e lances e de julgamento, os documentos de habilitação anteriormente inserida(s) no sistema, até a abertura da sessão pública;

7.9. Não haverá ordem de classificação na etapa de apresentação da proposta e dos documentos de habilitação pelo licitante, o que ocorrerá somente após os procedimentos de abertura da sessão pública e da fase de envio de lances;

7.10. Serão disponibilizados para acesso público os documentos que compõem a proposta dos licitantes convocados para apresentação de propostas, após a fase de envio de lances;

7.11. Desde que disponibilizada a funcionalidade no sistema, o licitante poderá parametrizar o seu valor final mínimo quando do cadastramento da proposta e obedecerá às seguintes regras:

7.11.1. a aplicação do intervalo mínimo de diferença de valores entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta; e

7.11.2. os lances serão de envio automático pelo sistema, respeitado o valor final mínimo estabelecido e o intervalo de que trata o subitem acima;

7.12. O valor final mínimo parametrizado no sistema poderá ser alterado pelo fornecedor durante a fase de disputa, sendo vedado:

7.12.1. valor superior a lance já registrado pelo fornecedor no sistema, quando adotado o critério de julgamento por menor preço; e

7.12.2. percentual de desconto inferior a lance já registrado pelo fornecedor no sistema, quando adotado o critério de julgamento por maior desconto;

7.13. Caberá ao licitante interessado em participar da licitação acompanhar as operações no sistema eletrônico durante o processo licitatório e se responsabilizar pelo ônus decorrente da perda de negócios diante da inobservância de mensagens emitidas pela Administração ou de sua desconexão;

7.14. O licitante deverá comunicar imediatamente ao provedor do sistema qualquer acontecimento que possa comprometer o sigilo ou a segurança, para imediato bloqueio de acesso;

8. DO PREENCHIMENTO DA PROPOSTA

8.1. O formulário de proposta de preços, em sua forma impressa, conforme modelo do Anexo II deste Edital, somente será utilizado pelo licitante vencedor com vistas à readequação de sua oferta final, devendo constar;

8.1.1. O número do item, a quantidade, a unidade, a especificação, o preço unitário e total com no máximo 2 (duas) casas decimais após a vírgula;

8.1.2. As condições de execução dos serviços e pagamento atenderão ao disposto no Termo de Referência, Anexo I deste Edital;

8.1.3. Prazo de validade da proposta de 60 (sessenta) dias, contados da data de realização da sessão pública do pregão;

8.2. Todas as especificações do objeto contidas na proposta vinculam o licitante;

8.3.Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente no objeto;

8.4.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;

8.5.Qualquer elemento que possa identificar a licitante, antes da finalização da etapa de lances, importará na desclassificação da proposta.

8.6.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 o objeto licitado nos seus termos;

8.7.Os licitantes devem respeitar os preços máximos estabelecidos na estimativa elaborada para esta licitação;

8.8.Se por motivo de força maior, a adjudicação não puder ocorrer dentro do período de validade da proposta, e caso, persista o interesse da Administração na esta poderá solicitar a prorrogação da validade da proposta por igual prazo

9. DA ABERTURA DA SESSÃO PÚBLICA E CLASSIFICAÇÃO DAS PROPOSTAS

9.1.A abertura da sessão pública deste PREGÃO ELETRÔNICO, conduzida pelo pregoeiro, ocorrerá automaticamente pelo sistema na data e hora indicadas no preâmbulo deste edital, no endereço eletrônico **www.novobbmnet.com.br**;

9.2.A comunicação entre o pregoeiro e as licitantes ocorrerá mediante troca de mensagens, em campo próprio do sistema eletrônico (chat), vedada outra forma de comunicação;

9.3.Cabe à licitante acompanhar as operações e convocações durante a sessão pública até o encerramento definitivo no sistema eletrônico, ficando responsável pelo ônus decorrente da perda de negócios diante da inobservância de qualquer mensagem emitida pelo sistema ou de sua desconexão;

9.4.Será desclassificada a proposta que identifique o licitante;

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

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

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

9.8.Na hipótese de o sistema eletrônico se desconectar no decorrer da etapa de envio de lances da sessão pública e permanecer acessível aos licitantes, os lances continuarão sendo recebidos, sem prejuízo dos atos realizados;

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

9.10. Na hipótese de necessidade da suspensão da sessão pública para a realização de diligências, com vistas ao saneamento de Propostas e documentos de Habilitação de que tratam os artigos 41 e 42 da Lei Federal 14.133/2021, o seu reinício somente poderá ocorrer mediante aviso prévio no sistema com, no mínimo, 24hs (vinte e quatro horas) de antecedência, e a ocorrência será registrada em ata;

10. MODO DE DISPUTA E FORMULAÇÃO DE LANCES

10.1. Será adotado neste pregão eletrônico o modo de disputa aberto, em que os licitantes apresentarão lances públicos e sucessivos, observando o critério de julgamento definido para a licitação, conforme preâmbulo deste Edital;

10.2. Aberta a etapa competitiva, os licitantes classificados poderão encaminhar lances, exclusivamente por meio do sistema eletrônico, sendo imediatamente informadas pelo sistema do recebimento e do valor consignado no registro;

10.3. Os licitantes somente poderão oferecer valor inferior ao último lance por ele ofertado e registrado pelo sistema, observando, o intervalo mínimo de diferença de valores de R$ 0,01 (um centavo), entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta;

10.4. Os licitantes somente poderão ofertar lances inferiores ao último por eles ofertado e registrado no sistema;

10.5. Os licitantes poderão, ainda, apresentar lances superiores ao lance melhor classificado, porém inferiores ao último lance dado pelo próprio licitante;

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

10.7. Durante o transcurso da sessão, as licitantes serão informadas pelo sistema, em tempo real, do valor do menor lance registrado, vedada a identificação da ofertante;

10.8. Durante o transcurso da sessão, as licitantes serão informadas pelo sistema, em tempo real, do valor do menor lance registrado, vedada a identificação da ofertante;

10.9. O Pregoeiro poderá, durante a disputa, como medida excepcional, excluir a proposta ou o lance que possa comprometer, restringir ou frustrar o caráter competitivo do processo licitatório, mediante comunicação eletrônica automática via sistema;

10.10. Eventual exclusão de proposta do licitante, de que trata o item anterior, implica a retirada do licitante do certame, sem prejuízo do direito de defesa;

10.11. No modo de disputa ABERTO, os licitantes apresentarão lances públicos e sucessivos, com prorrogações;

10.12. A etapa de lances da sessão pública terá duração de 10 (dez) minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos dois minutos do período de duração da sessão pública;

10.13. A prorrogação automática da etapa de lances, de que trata o subitem anterior, será de dois minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários.

Prefeitura Municipal de Piraí – APROVADO – Assessoria Jurídica

Prefeitura Municipal de Piraí – Secretaria Municipal Administração – Estado do Rio

10.14. Não havendo novos lances na forma estabelecida nos itens anteriores, a sessão pública encerrar-se-á automaticamente, e o sistema ordenará e divulgará os lances conforme a ordem final de classificação.

10.15. No caso de ao final da etapa de lances, o primeiro colocado oferecer proposta acima do preço máximo, o pregoeiro deverá negociar junto ao mesmo, e em não havendo concordância do licitante, será declarado desclassificado;

10.16. Na ocorrência de insucesso na situação prevista no subitem anterior, o pregoeiro deverá dar continuidade na negociação, junto ao demais licitantes, respeitada a ordem de classificação ou, em caso de propostas intermediárias empatadas, serão utilizados os critérios de desempate definidos no artigo 60 da Lei Federal nº 14.133/2021;

10.17. Caso o licitante não apresente lances, concorrerá com o valor de sua proposta inicial;

10.18. Ao final da etapa competitiva, observada a prerrogativa das microempresas e empresas de pequeno porte previstas nos artigos 44 e 45 da Lei Complementar nº 123/2006, regulamentada pelo Decreto nº 8.538, de 2015, serão aplicados, caso necessário, os critérios de desempate previstos no artigo 60 da lei Federal nº 14.133/21;

10.19. Empatadas as propostas iniciais e não havendo o envio de lances após o início da fase competitiva, aplicam-se os critérios de desempate de que trata o artigo 60 da Lei Federal nº 14.133/21;

11. DOS BENEFÍCIOS DAS ME'S, EPP'S E EQUIPARADAS

11.1. 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 Lei Complementar nº 123, de 2006

12. DA NEGOCIAÇÃO E VERIFICAÇÃO DE IMPEDIMENTOS

12.1. Após o encerramento da etapa de lances, concedido o benefício do desempate às microempresas, empresas de pequeno porte e equiparadas eventualmente participantes, de que trata o artigo 44 da Lei Complementar nº 123/06, o pregoeiro deverá propor negociação direta com o licitante melhor classificado, objetivando obter condições mais vantajosas para a Administração, observado o critério de julgamento e o valor estimado para a contratação, não se admitindo negociar condições diferentes das previstas neste edital;

12.2. A negociação será realizada e registrada por meio do sistema **www.novobbmnet.com.br**, podendo ser acompanhada pelas demais licitantes, devendo o seu resultado ser formalmente anexado aos autos do processo de licitação;

12.3. Caso o licitante provisoriamente classificado em primeiro lugar tenha se utilizado de algum tratamento favorecido às ME/EPP, o pregoeiro verificará os impedimentos previstos no item 06;

12.4. Deverá ser observado, ainda, se o licitante atende às condições de participação no certame, relativamente às exigências previstas no item 05 deste edital, especialmente quanto à existência de sanção que impeça a sua participação ou a futura contratação, mediante a consulta ao seguinte cadastro:

12.4.1. Certidão Negativa Correcional – Entes Privados (e-PAD, CGU-PJ, CEIS, CNEP e CEPIM). (http://cgu.gov.br)

12.5. A consulta realizar-se-à em nome da sociedade empresária licitante e, também, de seu sócio majoritário, por força do artigo 12 da Lei Federal nº 8.429/92, 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;

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

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

12.8. O fornecedor será convocado para manifestação previamente a uma eventual desclassificação (IN nº 3/2018, art. 29, §2º)

12.9. Constatada a existência de sanção, a licitante será considerada desclassificada, por falta de condição de participação;

12.10. Caso atendidas as condições de participação, será iniciado o procedimento de habilitação.

13. DA CONFORMIDADE E ACEITAÇÃO DA PROPOSTA MELHOR CLASSIFICADA

13.1. Verificadas as condições de participação e de utilização do tratamento favorecido, o pregoeiro examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação aos valores máximo e unitário estipulado para contratação neste Edital e em seus anexos;

13.2. Como critério para a análise da conformidade das propostas serão observados os requisitos do TERMO DE REFERÊNCIA – ANEXO I e do MODELO DE PROPOSTA DE PREÇOS – ANEXO II deste edital;

13.3. Como critério de aceitabilidade de preços das propostas será(ão) adotado(s) o(s) preço(s) unitário(s) estimado(s), ou seja, após encerrada a fase de lances não serão aceitas propostas cujo(s) preço(s) unitário(s) seja(m) superior(es) ao(s) estimado(s) no TERMO DE REFERÊNCIA – ANEXO I deste edital;

13.4. Será rejeitada a proposta que apresentar as seguintes inadequações:

13.4.1. contiver vícios insanáveis;

13.4.2. não obedecer às especificações técnicas contidas no Termo de Referência;

13.4.3. apresentar preços inexequíveis ou permanecerem acima do preço máximo definido para a contratação;

13.4.4. não tiverem sua exequibilidade demonstrada, quando exigido pela Administração;

13.4.5. apresentar desconformidade com quaisquer outras exigências deste Edital ou seus anexos, desde que insanável;

13.5. O licitante classificado em primeiro lugar deverá encaminhar a proposta comercial, com os respectivos valores readequados ao valor total vencedor e observando o limite máximo dos preços unitários estipulados no TERMO DE REFERÊNCIA – ANEXO I deste edital, no prazo a ser indicado, justificadamente, pelo pregoeiro, nunca inferior a 2 (duas) horas e contado da solicitação efetuada no sistema, devidamente assinada pelo seu responsável ou representante legal;

13.6. O prazo de encaminhamento da proposta readequada, ou de documentos complementares reputados de envio necessário, poderá ser prorrogado de ofício pelo Pregoeiro ou por solicitação do licitante, por igual período inicial, mediante justificativa aceita.

13.7. O Pregoeiro realizará a verificação da conformidade da proposta classificada em primeiro lugar quanto à adequação ao objeto estipulado e a compatibilidade do preço final em relação ao estimado para a contratação, inclusive os seus valores unitários, desclassificando ao final as que estiverem em desacordo com os requisitos estabelecidos neste edital;

13.8. Como critério de julgamento das propostas, será adotado o critério definido no preâmbulo deste edital;

13.9. Na verificação do preço final, deverá realizar a aferição da sua exeqüibilidade, considerando indícios de inaptidão as propostas inferiores a 50% (cinquenta por cento) do valor orçado para a licitação, na forma do artigo 34 da Instrução Normativa SEGES Nº 73/2022;

13.10. Na hipótese de que trata o item anterior, a inexequibilidade somente será considerada após diligência efetuada pelo Pregoeiro que resulte comprovação de que:

13.10.1. o custo do licitante ultrapassa o valor da proposta; e

13.10.2. inexistem custos de oportunidade capazes de justificar o vulto da oferta;

13.11. Pregoeiro poderá, no julgamento das propostas, sanar erros ou falhas que não alterem a sua substância e sua validade jurídica, atribuindo-lhes eficácia para fins de classificação;

13.12. Constatado o atendimento às exigências fixadas neste edital, a licitante será considerada classificada;

13.13. A desclassificação de proposta será fundamentada e registrada no sistema, sendo acompanhada, em tempo real, por todos os participantes;

14. DA FASE DE HABILITAÇÃO

14.1. O Pregoeiro observará o cumprimento das exigências de habilitação previstas nos itens 15 a 18, além da entrega e o cumprimento das obrigações a que se referem as declarações previstas neste edital de licitação;

14.2. Será exigida a apresentação dos documentos de habilitação apenas do licitante melhor classificado;

14.3. Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante apresentação dos documentos originais não digitais quando houver dúvida em relação à integridade do documento digital ou quando a lei expressamente o exigir;

14.4. Após a apresentação dos documentos de habilitação, fica vedada a substituição ou a apresentação de novos documentos, salvo em sede de diligência, para:

14.4.1. complementação de informações acerca dos documentos já apresentados pelos licitantes e desde que necessária para apurar fatos existentes à época da abertura do certame; e

14.4.2. atualização de documentos cuja validade tenha expirado após a data de recebimento das propostas;

14.5. Na hipótese de necessidade de envio de documentos complementares, estes deverão ser apresentados em formato digital, via sistema, no prazo mínimo de 2 (duas) duas horas, a ser definido, justificadamente, pelo Pregoeiro, contado da convocação efetuada no sistema, podendo ser prorrogado por igual período, nas situações elencadas no § 3º do artigo 29 da Instrução Normativa SEGES 73/2022;

14.6. A verificação do Pregoeiro em sítios eletrônicos oficiais de órgãos e entidades emissores de certidões constitui meio legal de prova, para fins de habilitação;

14.7. Na análise dos documentos de habilitação, o Pregoeiro poderá sanar erros ou falhas que não alterem a substância dos documentos e sua validade jurídica, mediante decisão fundamentada, registrada em ata e acessível a todos, atribuindo-lhes eficácia para fins de habilitação e classificação, conforme previsto no § 1º do artigo 64 da Lei Federal 14.133/21;

14.8. Serão disponibilizados para acesso público os documentos de habilitação dos licitantes convocados para a apresentação da documentação habilitatória, após concluídos os procedimentos de que trata o item anterior;

14.9. Na hipótese de o licitante não atender às exigências para habilitação, o pregoeiro, examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda ao edital de licitação;

14.10. A documentação deverá ter validade na data estabelecida no preâmbulo deste edital para a abertura da sessão. As certidões valerão nos prazos que lhes são próprios ou, inexistindo esse prazo, reputar-se-ão válidas por 90 (noventa) dias, contados de sua expedição;

14.11. As empresas estrangeiras que não funcionem no País deverão apresentar documentos equivalentes para atendimento de exigências de habilitação, inicialmente apresentados em tradução livre;

14.12. Na hipótese de o licitante vencedor ser empresa estrangeira que não funcione no País, para fins de assinatura do contrato, os documentos exigidos para a contratação serão traduzidos por tradutor juramentado no País e apostilados nos termos do disposto no Decreto nº 8.660, de 29 de janeiro de 2016, ou de outro que venha a substituí-lo, ou consularizados pelos respectivos consulados ou embaixadas;

15. HABILITAÇÃO JURÍDICA

15.1. Para fins de comprovação da habilitação jurídica, deverão ser apresentados, conforme o caso, os seguintes documentos:

15.1.1. Cédula de identidade e CPF dos sócios ou dos diretores;

Prefeitura Municipal de Piraí – APROVADO – Assessoria Jurídica

Prefeitura Municipal de Piraí – Secretaria Municipal Administração – Estado do Rio

15.1.2. Empresário Individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

15.1.3. Sociedade Simples: Registro no Registro Civil das Pessoas Jurídicas do local de sua sede, acompanhada de documento probatório de seus administradores;

15.1.4. Microempreendedor Individual–MEI: Certificado da Condição de Microempreendedor Individual – CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio https://www.gov.br/empresas-e-negocios/pt-br/empreendedor;

15.1.5. Sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada – EIRELI: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

15.1.6. No caso de sociedades por ações, será necessária a apresentação conjunta de documentos de eleição de seus administradores e alterações ou da consolidação respectiva;

15.1.7. Filial, sucursal ou agência de sociedade simples ou empresária: inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz;

15.1.8. Sociedade empresária estrangeira: portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução Normativa DREI/ME nº 77, de 18 de março de 2020;

15.2. Os documentos apresentados deverão indicar os responsáveis pela Administração e estar acompanhados de todas as alterações ou da consolidação respectiva;

16. REGULARIDADE FISCAL, SOCIAL E TRABALHISTA

16.1. Prova de inscrição ou no Cadastro Nacional da Pessoa Jurídica do Ministério da Fazenda – CNPJ/MF

16.2. Prova de inscrição no Cadastro de Contribuições Estadual e/ou Municipal, conforme o caso, relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto licitado;

16.3. Prova de regularidade com a Seguridade Social (INSS), através da apresentação da Certidão Conjunta Negativa de Débitos relativos a Tributos Federais e à Dívida Ativa da União, ou Positiva com Efeito de Negativa, expedida pela Secretaria da Receita Federal do Brasil (RFB) e Procuradoria Geral da Fazenda Nacional (PGFN), que abrange, inclusive, as contribuições sociais previstas nas alíneas “a” a “d”, do parágrafo único, do artigo 11, da Lei Federal nº 8.212, de 1991, comprovando a inexistência tanto de débitos inscritos quanto de não inscritos na Dívida Ativa da União;

16.4. Prova de regularidade com a Fazenda [Estadual/Distrital] e [Municipal/Distrital] do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;

16.4.1. Fazenda Estadual: apresentação da Certidão Negativa de Débitos, ou Certidão Positiva com efeito de Negativa, do Imposto sobre Operações relativas à Circulação de Mercadorias e sobre Prestações de Serviços de Transporte Interestadual, Intermunicipal e de Comunicação – ICMS, expedida pela Secretaria de Estado de Fazenda, e da Procuradoria Geral do Estado com relação a débitos inscritos em Dívida Ativa, quando for o caso;

16.4.2. Fazenda Municipal: apresentação da Certidão Negativa de Débitos, ou Certidão Positiva com efeito de Negativa, do Imposto sobre Serviços de Qualquer Natureza – ISS, apresentação da Certidão Negativa de Débitos com relação ao IPTU, e da Procuradoria Geral do Município com relação a débitos inscritos em Dívida Ativa, quando for o caso;

16.5. Prova de regularidade perante o Fundo de Garantia por Tempo de Serviço (FGTS), mediante apresentação do Certificado de Regularidade do FGTS – CRF, expedido pela Caixa Econômica Federal – CEF;

16.6. Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de Certidão Negativa de Débitos Trabalhistas (CNDT) ou da Certidão Positiva de Débitos Trabalhistas com os mesmos efeitos da CNDT;

16.7. Na hipótese de tratar-se de microempreendedor individual, microempresa ou de empresa de pequeno porte, na forma da lei, não obstante a obrigatoriedade de apresentação de toda a documentação habilitatória, a comprovação da regularidade fiscal e trabalhista somente será exigida para efeito de assinatura do contrato caso se sagre vencedora na licitação;

16.7.1. Os MEI/ME/EPP deverão apresentar os documentos elencados na Regularidade Fiscal e Trabalhista deste Pregão Eletrônico, mesmo que apresentem alguma restrição;

16.7.2. Havendo alguma restrição na comprovação da regularidade fiscal e trabalhista exigidas neste Edital, será(ão) assegurado(s) ao(s) microempreendedores individuais, à(s) microempresa(s) e empresa(s) de pequeno porte adjudicatária(s) deste certame o prazo de 5 (cinco) dias úteis, contados a partir do momento em que for(em) declarada(s) a(s) vencedora(s), prorrogável por igual período, a critério da Administração municipal, para a regularização da documentação, pagamento ou parcelamento do débito, e emissão de eventuais certidões negativas ou positivas com efeito de certidão negativa;

16.7.3. A não regularização da documentação, no prazo previsto, implicará decadência do direito à(s) contratação(ões), sem prejuízo das sanções previstas nos artigos 155 e 156 da Lei 14.133/2021, sendo facultado à Administração convocar as licitantes remanescentes, na ordem de classificação, para celebrar (em) a(s) contratação(ões), ou revogar a licitação;

17. QUALIFICAÇÃO ECONÔMICO-FINANCEIRA

17.1. Apresentação de certidões negativas de feitos sobre falência expedidas pelos distribuidores da sede da pessoa jurídica, ou de execução patrimonial, expedida no domicílio da pessoa física;

17.1.1. As certidões deverão vir acompanhadas de declaração oficial da autoridade judiciária competente, relacionando os distribuidores que, na Comarca de sua sede, tenham atribuição para expedir certidões negativas de falências e recuperação judicial, ou de execução patrimonial;

17.1.2. Ficam dispensadas da apresentação da certidão do item anterior, as empresas sediadas nos Estados onde a certidão de falências é emitida pelo Tribunal de Justiça e engloba a distribuição em todas as comarcas do Estado;

17.2. As empresas que estiverem em recuperação judicial ou extrajudicial deverão apresentar o plano de recuperação devidamente homologado pelo juízo competente.

18. QUALIFICAÇÃO TÉCNICA

18.1. O fabricante da solução deverá fornecer, obrigatoriamente, uma carta oficial de parceria emitida diretamente pelo fabricante, atestando a validade e a categoria da parceria, não sendo aceitos prints de informações provenientes de sites ou outras fontes não oficiais. A carta de parceria deverá ser datada, assinada por representante autorizado do fabricante.

18.2. Também comprovar que possui no mínimo 01 (um) especialista na solução de firewall e endpoint ofertadas, por meio de certificações da fabricante, que integre a equipe de trabalho, para assegurar o pleno funcionamento e a eficiência operacional do projeto, contribuindo para a continuidade dos serviços de tecnologia da informação oferecidos.

18.3. Deve apresentar a comprovação (declaração) emitida pelo fabricante do software ofertado, declarando que a empresa licitante está autorizada a comercializar e gerenciar as subscrições ofertadas para este Certame.

18.4. Para fins de comprovação de aderência do equipamento ofertado, caso haja necessidade poderá ser solicitada ao licitante a apresentação de documento (ponto a ponto) que indique a devida descrição de cada item que compõe o termo de referência, juntamente com a proposta, indicando no manual/catálogo do fabricante a aderência do produto aos requisitos das especificações técnicas.

18.5. A empresa licitante deverá comprovar sua capacidade técnica, por meio da apresentação de atestado(s) de capacidade técnica emitidos por pessoas jurídicas de direito público ou privado, que comprovem o fornecimento de produtos pertinentes e compatíveis, e confirmem a execução de serviços similares ao objeto da licitação.

19. DOS RECURSOS

19.1. A interposição de recurso referente ao julgamento das propostas, à habilitação ou inabilitação de licitantes, à anulação ou revogação da licitação, observará o disposto no art. 165 da Lei nº 14.133, de 2021;

19.2. O prazo recursal é de 3 (três) dias úteis, contados da data de intimação ou de lavratura da ata;

19.3. No que concerne as decisões proferidas nesta licitação, qualquer licitante poderá, no prazo máximo de 15 (quinze) minutos, a ser concedido pelo Pregoeiro, após o respectivo término do julgamento das propostas e do ato de habilitação ou inabilitação, em campo próprio do sistema, manifestar sua intenção de recorrer, sob pena de preclusão, ficando a autoridade superior autorizada a adjudicar o objeto ao licitante declarado vencedor no caso de inexistência de manifestação;

19.4. As razões do recurso deverão ser apresentadas em momento único, em campo próprio no sistema, no prazo de três dias úteis, contados a partir da data de intimação via sistema;

19.5. Os demais licitantes ficarão intimados para se desejarem, apresentar suas contrarrazões, no prazo de três dias úteis, contado a partir do dia útil seguinte ao final do prazo de apresentação das razões recursais;

19.6. Os recursos e as contrarrazões serão dirigidos ao Pregoeiro que proferiu a decisão recorrida, que, se não reconsiderar o ato ou a decisão no prazo de 3 (três) dias úteis, o encaminhará, relatando suas razões de forma fundamentada e motivada, a AUTORIDADE SUPERIOR, que deverá proferir sua decisão no prazo máximo de 10 (dez) dias úteis, contado do recebimento dos autos;

19.7. O recurso terá efeito suspensivo do ato ou da decisão recorrida, até que sobrevenha decisão final da autoridade competente;

19.8. Decididos os recursos e constatada a regularidade dos atos praticados, AUTORIDADE SUPERIOR adjudicará o objeto e homologará a licitação, caso não seja necessário o retorno da licitação à fase de lances;

19.9. Será assegurado ao licitante vista dos elementos indispensáveis à defesa de seus interesses;

19.10. O acolhimento do recurso importará a invalidação apenas dos atos insuscetíveis de aproveitamento

20. DO INSTRUMENTO CONTRATUAL

20.1. A licitante vencedora será convocada para assinar o contrato ou retirar a nota de empenho, no prazo de 5 (cinco) dias úteis;

20.2. A convocação a que se refere o subitem anterior far-se-á através de comunicação endereçada diretamente à licitante vencedora, dentro do prazo de validade de sua proposta;

20.3. O prazo estabelecido no documento da convocação poderá ser prorrogado uma vez, por igual período, quando solicitado expressamente pela parte durante o seu transcurso e se acolhidas pela Administração as justificativas apresentadas;

20.4. Para a formalização do contrato e/ou emissão da nota de empenho, o licitante vencedor deverá manter as mesmas condições de habilitação consignadas neste edital;

20.5. O presente edital e seus anexos e a proposta do adjudicatário serão partes integrantes do contrato ou nota de empenho de despesa, a qual substituirá o instrumento de contrato independe de transcrição;

20.6. A recusa injustificada do adjudicatário em assinar o contrato ou retirar a nota de empenho, até 05 (cinco) dias úteis após sua convocação, caracteriza o descumprimento total da obriga-

ção, sujeitando-o às penalidades legalmente estabelecidas, e facultando ao Município convocar os licitantes remanescentes, obedecida a ordem de classificação ou revogar a licitação;

20.7. Na hipótese de o vencedor da licitação não retirar o instrumento equivalente no prazo e nas condições estabelecidas, o pregoeiro realizará a reabertura do pregão, examinando as ofertas subsequentes e a qualificação dos licitantes, na ordem de classificação, até a apuração de uma que atenda e proporcione a viabilização da contratação, nas condições propostas pelo licitante vencedor;

20.8. Caso nenhum dos licitantes aceite a contratação nos termos do subitem anterior, a Administração, observados o valor estimado e sua eventual atualização nos termos do edital de licitação, poderá:

20.8.1. convocar os licitantes remanescentes para negociação, na ordem de classificação, com vistas à obtenção de preço melhor, mesmo que acima do preço ou inferior ao desconto do adjudicatário;

20.8.2. adjudicar e celebrar o contrato nas condições ofertadas pelos licitantes remanescentes, atendida a ordem classificatória, quando frustrada a negociação de melhor condição;

20.9. As sanções administrativas mencionadas no item 25 não serão aplicáveis aos licitantes remanescentes convocados na forma do subitem 20.8.1;

20.10. O contrato não poderá ser objeto de cessão, subcontratação ou transferência, no todo ou em parte

21. DA GESTÃO E FISCALIZAÇÃO DO CONTRATO

21.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas, e cada parte responderá pelas consequências de sua inexecução total ou parcial;

21.2. A execução do contrato será acompanhada e fiscalizada por servidor(es) indicado pelo órgão solicitante e designado(s) em portaria;

21.3. O fiscal do contrato anotará em registro próprio todas as ocorrências relacionadas à execução do contrato, determinando o que for necessária para regularização da falta ou defeitos observados.

21.4. As comunicações entre Contratante e Contratada devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim;

21.5. O fiscal do contrato informará, em tempo hábil, ao superior do seu órgão, divisão ou setor, a situação que demandar decisão ou providência que ultrapasse a sua competência;

21.6. O fiscal do contrato será auxiliado pelos órgãos de assessoramento jurídico e de controle interno da Administração, que deverá dirimir dúvidas e subsidiá-lo com informações relevantes para prevenir riscos na execução contratual;

21.7. A contratante poderá convocar representante da Contratada para adoção de providências que deixem de ser cumpridas de imediato;

21.8. O contratado será responsável pelos danos causados diretamente à Administração ou a terceiros em razão da execução do contrato, e não excluirá nem reduzirá essa responsabilidade a fiscalização ou o acompanhamento pelo contratante;

21.9. O contratado fica obrigado a aceitar nas mesmas condições contratuais, os acréscimos ou diminuição quantitativa de seu objeto, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato;

21.10. As alterações contratuais deverão ser formalizadas por termo aditivo, exceto registros que não caracterizam alteração no contrato, que poderão ser formalizados por simples apostila, de acordo com as situações previstas no art. 136 da Lei Federal nº 14.133/2021.

22. MODELO DE EXECUÇÃO DO OBJETO

22.1. CONDIÇÕES DE EXECUÇÃO DO SERVIÇO:

22.1.1. Os serviços, objeto deste edital, deverão ser executados atendendo todas as especificações contidas no Termo de Referência, anexo I deste edital, independente de transcrição;

22.1.2. O licitante vencedor fica obrigado a manter, durante toda a execução do contrato, em compatibilidade com as obrigações por ele assumidas, todas as condições exigidas para a habilitação no presente edital;

22.2. CONDIÇÕES DE RECEBIMENTO DO OBJETO

22.2.1. Os serviços objeto deste Termo de Referência serão recebidos e aceitos, de acordo com o art. 140 da lei nº 14.133/2021, provisoriamente, após sumária inspeção realizada pela Fiscalização da Secretaria responsável, para posterior verificação da qualidade e conformidade do objeto às especificações técnicas exigidas neste termo, podendo ser rejeitados caso não estejam conforme as especificações estabelecidas;

22.2.2. A contratada deverá dar total garantia quanto à qualidade dos serviços executados, ficando obrigada a reparar, corrigir ou substituir às suas expensas, no total ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções comprovadamente fora das especificações técnicas discriminadas no presente termo;

22.2.3. O objeto será recebido definitivamente no prazo de 15 (quinze) dias, contados do recebimento provisório, por servidor ou comissão designada para fiscalização, mediante termo detalhado que comprove o atendimento das condições e especificações discriminadas no Termo de Referência.

23. DAS CONDIÇÕES DO PAGAMENTO

23.1. O pagamento será realizado, de acordo com os serviços efetivamente executados e atestados pela fiscalização, 30 (trinta) dias após o adimplemento do objeto, assim considerada a execução do serviço, acompanhada do respectivo documento de cobrança (nota fiscal/fatura) devidamente atestada pela Fiscalização;

23.2. Os pagamentos serão efetuados, obrigatoriamente, por meio de crédito em conta corrente, cujo número e agência deverão ser informados pelo adjudicatário até a assinatura do contrato;

23.3. Os prestadores de Serviço e fornecedores de bens, deverão emitir as notas fiscais em observância ás regras de retenção, dispostas na Instrução Normativa RFB n° 1234, de 11 de janeiro de 2012, sob pena de não aceitação.

23.4. A retenção do imposto de renda deverá ser destacada no corpo do documento fiscal observando os percentuais estabelecidos no anexo I da Instrução Normativa RFB nº 1.234/2012.

23.5. As pessoas jurídicas amparadas por isenção, não incidência ou alíquota zero devem informar essa condição no documento fiscal, inclusive o enquadramento legal, sob pena de, se não o fizerem, sujeitarem-se à retenção do imposto de renda sobre o valor total do documento correspondente à natureza do bem ou serviço

23.6. Havendo erro na apresentação da nota fiscal ou instrumento de cobrança equivalente, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus ao contratante;

23.7. Em caso de atraso injustificado no pagamento, o valor será compensado financeiramente em 0,5% (cinco décimos por cento) de juros de mora por mês "pro rata tempore", contados a partir do dia seguinte ao seu vencimento até a data do efetivo pagamento;

24. DAS IRREGULARIDADES E SANÇÕES ADMINISTRATIVAS

24.1. O licitante/adjudicatário participante do procedimento licitatório estará sujeito, durante o seu transcorrer, à aplicação das seguintes sanções administrativas previstas no artigo 156 da Lei Federal nº 14.133/21:

24.1.1. Advertência;

24.1.2. Multa;

24.1.3. Impedimento de Licitar e Contratar;

24.1.4. Declaração de inidoneidade para licitar ou contratar, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida sua reabilitação perante a própria autoridade que aplicou a penalidade;

24.2. Estarão passiveis das sanções previstas no item anterior, os licitantes que, com dolo ou culpa, se enquadrarem nas seguintes situações:

24.2.1. declarado inidôneo ou impedido de licitar e contratar com a Administração Pública Estadual, que se apresente para participar de procedimento licitatório;

24.2.2. venha frustrar ou fraudar, com o intuito de obter para si ou para outrem vantagem decorrente da adjudicação do objeto da licitação, o caráter competitivo do processo licitatório;

24.2.3. afaste ou tente afastar licitante por meio de violência, grave ameaça, fraude ou oferecimento de vantagem de qualquer tipo;

24.2.4. devasse o sigilo de proposta apresentada em processo licitatório ou proporcionar a terceiro o ensejo de devassá-lo;

24.2.5. patrocine, direta ou indiretamente, interesse privado perante a Administração Pública, dando causa à instauração de licitação ou à celebração de contrato cuja invalidação vier a ser decretada pelo Poder Judiciário;

24.2.6. deixe de entregar a documentação exigida para o certame ou não entregar qualquer documento que tenha sido solicitado pelo Pregoeiro;

24.2.7. não mantenha a proposta, dentro prazo de sua validade, salvo em decorrência de fato superveniente devidamente justificado, em especial quando:

24.2.7.1. não enviar a proposta adequada ao último lance ofertado ou após a negociação;

24.2.7.2. recusar-se a enviar o detalhamento da proposta quando exigível;

24.2.7.3. pedir para ser desclassificado quando encerrada a etapa competitiva;

24.2.7.4. apresentar proposta ou amostra em desacordo com as especificações do edital;

24.2.8. não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

24.2.9. recusar-se, sem justificativa, a assinar o contrato, ou a aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração;

24.2.10. apresente declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação:

24.2.11. fraude a licitação;

24.2.12. comporte-se de modo inidôneo ou cometa fraude de qualquer natureza, em especial quando:

24.2.12.1. agir em conluio ou em desconformidade com a lei;

24.2.12.2. induzir deliberadamente a erro no julgamento;

24.2.12.3. apresentar amostra falsificada ou deteriorada;

24.2.12.4. venha impedir, perturbar ou fraudar a realização de qualquer ato de procedimento licitatório público;

24.2.12.5. crie, de modo fraudulento ou irregular, pessoa jurídica para participar de licitação pública;

24.2.12.6. obtenha vantagem ou benefício indevido, de modo fraudulento, de modificações ou prorrogações de contratos celebrados com a administração pública, sem autorização em lei, no ato convocatório da licitação pública ou nos respectivos instrumentos contratuais;

24.3. Na aplicação das sanções, conjugadas as diretrizes do §1º do artigo 156 da Lei Federal nº 14.133/21, será observado o princípio da proporcionalidade, considerando-se especialmente:

24.3.1. a natureza e a gravidade da infração cometida;

24.3.2. as peculiaridades do caso concreto;

24.3.3. as circunstâncias agravantes ou atenuantes;

24.3.4. os danos para a Administração;

24.3.5. a vantagem auferida ou pretendida pelo infrator;

24.3.6. a consumação ou não da infração;

24.3.7. o grau de lesão ou perigo de lesão;

24.3.8. o efeito negativo produzido pela infração;

24.3.9. a cooperação da pessoa jurídica para a apuração das infrações;

24.3.10. a existência de mecanismos e procedimentos internos de integridade, auditoria e incentivo à denúncia de irregularidades e a aplicação efetiva de códigos de ética e de conduta no âmbito da pessoa jurídica;

24.4. A sanção de impedimento de licitar e contratar será aplicada ao responsável em decorrência das infrações administrativas relacionadas nos itens 25.2.1 e 25.2.6 a 25.2.8, quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo a qual pertencer o órgão ou entidade, pelo prazo máximo de 3 (três) anos;

24.5. Poderá ser aplicada ao responsável a sanção de declaração de inidoneidade para licitar ou contratar, em decorrência da prática das infrações dispostas nos itens 25.2.2 a 25.2.5 e 25.2.10 a 25.2.12, bem como pelas infrações administrativas previstas nos itens 25.2.1 e 25.2.6 a 25.2.8, que justifiquem a imposição de penalidade mais grave que a sanção de impedimento de licitar e contratar, cuja duração observará o prazo previsto no art. 156, §5º, da Lei nº 14.133/2021;

24.6. A multa será recolhida em percentual de 20% incidente sobre o valor estimado da licitação ou do valor proposto ou do(s) item(s) prejudicado(s) pela conduta do licitante, recolhida no prazo máximo de 30 (trinta) dias úteis, a contar da comunicação oficial;

24.7. Para as infrações previstas nos itens 25.2.1 e 25.2.6 a 25.2.8, a multa será de 10% sobre o valor estimado da licitação ou do valor proposto ou do(s) item(s) prejudicado(s) pela conduta do licitante;

24.8. Para as infrações previstas nos itens 25.2.2 a 25.2.5 e 25.2.9 a 25.2.13, a multa será de 20% sobre o valor estimado da licitação ou do valor proposto ou do(s) item(s) prejudicado(s) pela conduta do licitante;

24.9. A multa poderá ser aplicada cumulativamente com as sanções de Advertência, Impedimento de Licitar e Contratar, e com a Declaração de Inidoneidade de Licitar ou Contratar;

24.9.1. Na aplicação da sanção de multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua notificação;

24.10. A recusa injustificada do adjudicatário em assinar o contrato, ou em aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração, caracterizará o descumprimento total da obrigação assumida e o sujeitará às penalidades e à imediata perda da garantia de proposta em favor do órgão ou entidade promotora da licitação, nos termos do art. 45, §4º da IN SEGES/ME nº 73, de 2022;

24.11. Decorridos 20 (vinte) dias da convocação para assinatura do contrato (ou retirada/aceite de empenho ou instrumento equivalente), sem a manifestação do adjudicatário, ficará configurada a referida recusa;

24.12. 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 os procedimentos previstos na Lei Federal nº 14.133/21;

24.13. A apuração de responsabilidades relacionadas às sanções de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar demandará a instauração de processo de responsabilização a ser conduzido por comissão composta por 2 (dois) ou mais servidores estáveis, que avaliará fatos e circunstâncias conhecidos e intimará o licitante ou o adjudicatário para, no prazo de 15 (quinze) dias úteis, contado da data de sua intimação, apresentar defesa escrita e especificar as provas que pretenda produzir;

24.14. Caberá recurso no prazo de 15 (quinze) dias úteis da aplicação das sanções de advertência, multa e impedimento de licitar e contratar, contado da data da intimação, o qual será dirigido à autoridade que tiver proferido a decisão recorrida, que, se não a reconsiderar no prazo de 5 (cinco) dias úteis, encaminhará o recurso com sua motivação à autoridade superior, que deverá proferir sua decisão no prazo máximo de 20 (vinte) dias úteis, contado do recebimento dos autos;

24.15. Caberá a apresentação de pedido de reconsideração da aplicação da sanção de declaração de inidoneidade para licitar ou contratar no prazo de 15 (quinze) dias úteis, contado da data da intimação, e decidido no prazo máximo de 20 (vinte) dias úteis, contado do seu recebimento;

24.16. O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente;

24.17. A aplicação das sanções previstas neste edital não exclui, em hipótese alguma, a obrigação de reparação integral dos danos causados a Município de Piraí;

24.18. As sanções administrativas aplicáveis por atos praticados no decorrer da execução contratual estão previstas no Termo de Referência e/ou na Minuta do Contrato, que constituem anexos deste Edital de Licitação;

25. DA IMPUGNAÇÃO AO EDITAL E DOS PEDIDOS DE ESCLARECIMENTOS

25.1. Qualquer pedido de esclarecimento ou de impugnação deverá ser enviado eletronicamente ao pregoeiro no endereço **www.novobbmnet.com.br**, até 3 (três) dias úteis anteriores à data fixada no edital para abertura da sessão pública, observado o horário limite de expediente diurno às 17:00 horas;

25.2. O pregoeiro responderá aos pedidos de esclarecimentos e/ou impugnação no prazo de até três dias úteis contados da data de recebimento do pedido, limitado ao último dia útil anterior à data da abertura do certame, e poderá requisitar subsídios formais aos responsáveis pela elaboração do edital de licitação e dos anexos, além de pronunciamentos de ordem técnica junto ao setor requisitante do objeto licitado;

25.3. A impugnação não possui efeito suspensivo, sendo a sua concessão medida excepcional que deverá ser motivada pelo pregoeiro, nos autos do processo de licitação;

Prefeitura Municipal de Piraí – APROVADO – Assessoria Jurídica

Prefeitura Municipal de Piraí – Secretaria Municipal Administração – Estado do Rio

25.4. Acolhida a impugnação contra o edital de licitação, será definida e publicada nova data para realização do certame, observado o prazo de ancoragem específico, conforme artigo 55 da Lei Federal 14.133/2021;

25.5. As respostas aos pedidos de esclarecimento e de impugnação serão divulgadas, concomitantemente nos endereços eletrônicos conforme item 1.3 do edital e **www.novobbmnet.com.br**, para conhecimento geral e dos interessados em participar da licitação, e vincularão os participantes e a Administração quanto ao seu conteúdo;

25.6. Eventuais modificações no edital de licitação implicarão nova divulgação na mesma forma de sua divulgação inicial, além do cumprimento dos mesmos prazos dos atos e procedimentos originais, exceto se, inquestionavelmente, a alteração não comprometer a formulação das propostas, resguardado o tratamento isonômico aos licitantes

26. DAS DISPOSIÇÕES GERAIS

26.1. 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;

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

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

26.4. 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;

26.5. 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;

26.6. Na contagem dos prazos estabelecidos neste edital, excluir-se-á o dia do início e incluir-se-á o do vencimento, iniciando-se e findando-se estes somente em dias de expediente na Administração;

26.7. O edital de licitação, e seus anexos, estarão disponíveis no Portal Nacional de Contratações Públicas (PNCP), no endereço eletrônico http://www.pirai.rj.gov.br/transparencia/contratoselicitações/ e www.novobbmnet.com.br, locais que disponibilização ainda o acompanhamento dos resultados das fases desta licitação;

26.8. Em caso de divergência entre normas infralegais e as contidas neste Edital, prevalecerão as últimas. Por outro lado, havendo divergência entre o Edital e o Termo de Referência, prevalecerá este;

26.9. Os casos omissos serão resolvidos pelo pregoeiro, com auxílio da equipe de apoio.

26.10. Para dirimir quaisquer dúvidas deste instrumento, que não possam ser solucionados administrativamente, fica eleito o Foro da cidade de Piraí/RJ, excluído qualquer outro.

Prefeitura Municipal de Piraí – APROVADO – Assessoria Jurídica

Prefeitura Municipal de Piraí – Secretaria Municipal Administração – Estado do Rio

27. DOS ANEXOS

27.1. Integram este edital os seguintes anexos

I. Termo de Referência
II. Modelo de Proposta de Preços
III. Minuta de Contrato

Piraí, 18 de agosto de 2026.

Secretaria Municipal de Administração

ANEXO I

TERMO DE REFERÊNCIA

1.OBJETO:

1.1. Aquisição de solução integrada (Harwdware/Software) de Firewall de Próxima Geração Tipo 1, conforme especificações e quantidades detalhadas neste Termo de Referência.

-

1.2. NATUREZA: material permanente e prestação de serviço.

1.2.1 Conforme disposto no art. 6º, XIII, da Lei n. 14.133/2021, os bens e serviços objeto do presente Termo de Referência classificam-se como bens e serviços comuns por apresentarem padrões de desempenho e qualidade que podem ser objetivamente definidos pelo edital, por meio de especificações usuais de mercado.

1.3. ESPECIFICAÇÃO E QUANTIDADE:

ITEM	UND.	QUANT.	DESCRIÇÃO	PREÇO UNIT.	PREÇO TOTAL
01	Unid.	01	Aquisição de Firewall Tipo 1 de Próxima Geração Tipo 1, com 24 meses de suporte e garantia de hardware.	R$ 86.000,00	R$ 86.000,00
02	Serv.	01	Pacote de licenças de Firewall para 12 meses renovável a cada 12 meses, IPS, Antivírus, Anti- spyware, Filtro de Web, Proteção contra ameaças avançadas, ZTNA, e firewall de aplicação web, Console de Gerência Administrativa e Centralização de Logs e Relatórios das soluções de Firewall para appliance de Firewall de Próxima Geração pelo prazo de 12 (doze) meses. Software para integração das soluções de Endpoint e do Firewall de próxima geração Tipo 1.	R$ 122.000,00	R$ 122.000,00

03	Unid.	01	Aquisição de 01 (um) dispositivo Ethernet Remotos, incluindo instalação, configuração e repasse de conhecimento, com 24 meses de suporte e garantia de hardware.	R$ 15.000,00	R$ 15.000,00
VALOR TOTAL=				**R$ 223.000,00**	

1.3.1. Os termos "possui", "permite", "suporta" e "é" implicam no fornecimento de todos os elementos necessários à adoção da tecnologia ou funcionalidade citada. O termo "ou" implica que a especificação técnica mínima dos serviços pode ser atendida por somente uma das opções. O termo "e" implica que a especificação técnica mínima dos serviços deve ser atendida englobando todas as opções.

1.3.2. Todos os equipamentos, produtos, peças e softwares necessários à prestação dos serviços deverão estar funcionando perfeitamente, sem vícios, não constar em listas de end-of-sale, end-of-support ou end-of-life do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante, com todas as funcionalidades exigidas neste Termo plenamente disponíveis durante toda a vigência do contrato. Já os softwares deverão, ainda, ser instalados em sua versão mais atualizada, e estar cobertos por contratos de suporte a atualização de versão do fabricante durante toda a vigência do respectivo serviço. Da mesma maneira, todo o hardware a ser utilizado na prestação dos serviços deverá estar coberto por garantia do fabricante.

1.3.3. Todos os componentes necessários à prestação dos serviços deverão ser compatíveis entre si, sem restrições aos requisitos constantes nestas especificações técnicas, e aos elencados do parque computacional atual.

1.3.4. A CONTRATADA deverá fornecer os equipamentos de TI em quantidades suficientes para atender as especificações técnicas mínimas dos serviços a serem ofertados, de acordo com as especificações técnicas mínimas.

1.3.5. A CONTRATADA deverá fornecer todos os equipamentos, softwares e tudo o mais que se fizer necessário para que todas as características e funcionalidades descritas neste termo funcionem plenamente.

1.3.6. A CONTRATADA deverá manter o CONTRATANTE atualizado sobre todos os fluxos adotados para a execução das atividades objeto da contratação do Software durante o período contratual, bem como sobre a forma de automatização de quaisquer serviços, documentando todos os procedimentos detalhadamente para que possam servir de base para a continuidade dos serviços independentemente da metodologia que possa ser adotada.

1.3.7. O Serviço de passagem de conhecimento Hands On da Solução deverá ser realizado no mínimo em dois momentos, inicialmente na implantação da solução e em outro momento a ser definido pela Gerência de Tecnologia da Informação, atendendo ao mínimo de intervalo de um ano entre uma passagem de conhecimento e outra.

1.4. VIGÊNCIA CONTRATUAL:

1.4.1 O prazo de prestação dos serviços objeto deste Termo de Referência será de 12 (doze) meses, a partir da ordem de serviço, podendo ter sua duração prorrogada a critério da Administração, tendo em vista tratar-se de serviço de natureza continuada de necessidade pública permanente a ser satisfeita, desde que os preços e condições sejam vantajosos para a Administração, nos termos do disposto no Art. 107, da Lei nº. 14.133/21.

2.FUNDAMENTAÇÃO DA CONTRATAÇÃO

2.1. A presente aquisição decorre da necessidade de assegurar a continuidade, a segurança e a confiabilidade dos serviços de tecnologia da informação utilizados pela Administração Pública, considerando a crescente dependência de sistemas informatizados para a execução das atividades institucionais, bem como o aumento dos riscos associados a incidentes de segurança da informação. A aquisição de Firewall de Próxima Geração mostra-se necessária para o a continuidade do adequado controle, monitoramento e proteção do tráfego de dados da rede corporativa, permitindo manter a implementação de mecanismos avançados de segurança, tais como prevenção contra intrusões, filtragem de conteúdo, inspeção de aplicações, proteção contra códigos maliciosos e registro centralizado de eventos. Trata-se de solução essencial para mitigação de riscos relacionados a acessos não autorizados, indisponibilidade de sistemas, comprometimento da integridade das informações e falhas de segurança que possam impactar a prestação dos serviços públicos.

2.2. A aquisição de 1 (um) Dispositivo Remoto Ethernet SD-WAN justifica-se pela necessidade de interligar unidades administrativas descentralizadas à rede principal de forma segura, padronizada e gerenciada centralmente. A utilização desses dispositivos possibilita a criação automática de conexões criptografadas, garantindo que as políticas de segurança definidas no ambiente central sejam aplicadas às unidades remotas, reduzindo riscos operacionais, custos com infraestrutura de comunicação dedicada e a necessidade de suporte técnico local especializado.

2.3. Com o uso do Equipamento de Conectividade Segura Remota é possível estender todas as políticas de segurança da sede para os pontos remotos, como unidades de saúde e escolas, garantindo que todos os acessos à rede estejam protegidos por firewall, filtragem de conteúdo, VPN segura, prevenção contra intrusões (IPS), antivírus, entre outras medidas.

2.4. Tem por finalidade atender às necessidades de Acesso á Internet e Sistemas nas Unidades de Saúde, Escolas e Prédios Administrativos de forma redundante. O link de Internet passa a ser transparente e sendo entregue por mais de uma operadora, proporcionando Failover como processo automático de transição para um sistema ou componente redundante (link de backup) quando o principal falha, garantindo a continuidade dos serviços sem interrupções. Essa funcionalidade é crucial para manter a alta disponibilidade de sistemas como servidores de banco de dados, redes e firewalls. O Failback fará com que o processo de retorne ao sistema original após o reparo. Com esta implantação minimiza-se o risco de parada na rede corporativa e garante o acesso de forma segura a Rede Corporativa passando pelo Firewall existente na Prefeitura e também atende as demandas de conformidade com a Lei do Marco Civil da Internet (Lei nº 12.965/2014) e a Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018).

2.5. Toda a gestão do Dispositivo de Extensão de Rede Segura deverá ser centralizada no firewall existente, o que elimina a necessidade de administrar múltiplos dispositivos em diferentes localidades, reduzindo custos operacionais e aumentando a segurança da informação. O Dispositivo de Comunicação Segura com a Sede elimina a necessidade de contratação de links dedicados (MPLS, por exemplo), pois funciona com conexões de internet convencionais (banda larga), estabelecendo automaticamente uma conexão segura com a sede por meio de túneis VPN criptografados. Isso reduz significativamente os custos com infraestrutura de rede entre as unidades.

2.6. As unidades de saúde, educação e administrativas do município dependem de sistemas informatizados para funcionamento adequado — como prontuários eletrônicos, sistemaseducacionais, acesso a sistemas do governo, entre outros. E o referido equipamento garante acesso seguro, confiável e de alta disponibilidade a esses serviços, minimizando riscos de falhas de segurança que possam comprometer dados sensíveis ou o funcionamento das atividades essenciais.

2.7. A aquisição de Equipamento de Conectividade Segura Remota permite uma padronização da conectividade segura em todas as unidades do município (ou estado), com possibilidade de expansão futura conforme necessidade. Essa abordagem padronizada facilita a manutenção, auditoria e conformidade com normas de segurança da informação, como a LGPD (Lei Geral de Proteção de Dados Pessoais).

2.8. A contratação de Software de Proteção Endpoint, integrado ao firewall e aos dispositivos remotos, é necessária para a proteção dos equipamentos finais utilizados no ambiente

institucional, prevenindo, detectando e respondendo a ameaças como vírus, ransomware, spyware e demais códigos maliciosos. A integração das soluções permite maior efetividade na identificação de incidentes, resposta coordenada a eventos de segurança e fortalecimento do controle sobre os ativos tecnológicos da Administração.

2.9. Diante do exposto, a aquisição de 1 Firewall Next Generation e 1 Dispositivo Ethernet Remoto para Redundância e a Contratação de Software de Proteção Remota por meio de processo licitatório se justifica plenamente, tanto do ponto de vista técnico quanto estratégico, garantindo segurança da informação, continuidade dos serviços públicos essenciais, otimização de recursos e alinhamento com a infraestrutura já implantada. Trata-se de uma medida necessária para garantir uma infraestrutura segura, escalável e eficiente para unidades descentralizadas da administração pública. Ressalta-se que a adoção integrada das soluções propostas contribui diretamente para o atendimento aos princípios da confidencialidade, integridade e disponibilidade da informação, bem como para a observância das obrigações legais impostas à Administração Pública, em especial aquelas previstas no Marco Civil da Internet (Lei nº 12.965/2014) e na Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018), no que se refere à adoção de medidas técnicas e administrativas aptas a proteger dados pessoais e reduzir riscos de incidentes de segurança.

3.DESCRIÇÃO DA SOLUÇÃO COMO UM TODO:

3.1. Solução de Segurança de Rede

3.1.1. Next-Generation Firewall (NGFW) para proteção de informação perimetral e de rede interna que inclui stateful firewall com capacidade para operar em alta disponibilidade (HA) em modo ativo-passivo ou ativo-ativo para controle de tráfego de dados por identificação de usuários e por camada 7, com controle de aplicação, administração de largura de banda (QoS), VPN IPsec e SSL, IPS, prevenção contra ameaças de vírus, malwares, Filtro de URL, criptografia de email, inspeção de tráfego criptografado e proteção de firewall de aplicação Web. Deverá ser fornecida console de gerenciamento dos equipamentos e centralização de logs em nuvem ou hardware específico ou virtualizado.

3.1.2. A console de gerenciamento em nuvem, deve estar no Brasil;

3.1.3. A console de gerenciamento deve ser possível atribuir configurações de concentradores de SD-WAN;

3.1.4. A console de gerenciamento deve dispor de configurações globais para replicação nos firewalls;

3.1.5. Deverão ser fornecidas as licenças para atualização de todos os componentes de software, vacinas de antivírus / malwares, endpoints, softwares de criptografia de armazenamento em nuvem e assinaturas de IPS, filtro de conteúdo web, controle de aplicações

e proteção de firewall de aplicação web sem custo adicional, pelo período mínimo de 12 (doze) meses.

3.1.6. Para os itens que representem bens materiais, a CONTRATADA deverá fornecer produtos novos, sem uso anterior.

3.1.7. Por cada appliance físico que compõe a plataforma de segurança, entende-se o hardware, software e as licenças necessárias para o seu funcionamento.

3.1.8. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico.

3.1.9. Deve possuir processadores próprios e para fins específicos, desenvolvidos exclusivamente pelo fabricante da solução, com a finalidade de processar tráfegos de redes e acelerar o processamento destes pacotes de redes, permitindo o uso de diversas funcionalidades de segurança ao mesmo tempo sem diminuir a performance do equipamento.

3.1.10. Todos os equipamentos de rede deverão possuir certificado de homologação expedido pela Agência Nacional de Telecomunicações (ANATEL).

3.1.11. Caso seja escolhida a opções por alta disponibilidade (HA) entende-se que a solução deverá ser composta ao menos por dois appliances, licenciados para funcionamento em redundância.

3.1.12. A solução deverá contemplar a totalidade das capacidades exigidas, sendo permitido o uso de mais de um equipamento (sempre em modo de alta disponibilidade HA) para complementar a solução, caso o fabricante não possua todas as funções em um único equipamento.

3.1.13. Caso a solução ofertada ofereça link dedicado para gerenciamento de HA, deverá suportar interfaces LAG e VLAN para o link HA dedicado e interfaces VLAN para links monitorados;

3.1.14. Cada appliance deverá ser capaz de executar a totalidade das capacidades exigidas para cada função, não sendo aceitos somatórias para atingir os limites mínimos.

3.1.15. O hardware e o software fornecidos não podem constar, no momento da apresentação da proposta, em listas de end-of-sale, end-of-support, end-of-engineering-support ou end-of-life do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante.

3.1.16. O firewall e a solução de endpoint deverão ser do mesmo fabricante, a fim de assegurar o gerenciamento centralizado e a padronização tecnológica durante a prestação dos serviços.

3.1.17. A exigência de que o firewall e a solução de endpoint sejam do mesmo fabricante visa garantir a integração nativa entre os componentes de segurança, possibilitando o gerenciamento centralizado, a padronização das políticas de proteção e a redução de falhas de compatibilidade durante a prestação dos serviços.

3.1.18. Essa padronização permite melhor visibilidade e controle unificado sobre os eventos de segurança, além de otimizar o desempenho, o suporte técnico e as atualizações. A utilização de soluções de fabricantes distintos poderia demandar camadas adicionais de integração, elevar custos operacionais e comprometer a eficiência do monitoramento e da resposta a incidentes.

3.1.19. Características específicas de desempenho e hardware do Firewall de próxima geração Tipo 1

3.1.20. Performance mínima de 58 Gbps de throughput para firewall.

3.1.21. Performance mínima de 14 Gbps de throughput de IPS.

3.1.22. Performance mínima de 12,5 Gbps de throughput para controle de NGFW.

3.1.23. Performance minima de 10 Gbps de Threat Protection throughput

3.1.24. Performance mínima de 31,1 Gbps de throughput de IPsec VPN.

3.1.25. Suporte a, no mínimo, 13.700.000 de conexões simultâneas.

3.1.26. Suporte a, no mínimo, 257.800 novas conexões por segundo.

3.1.27. Possuir o número irrestrito quanto ao máximo de usuários licenciados.

3.1.28. Possuir armazenamento interno em unidade de estado sólido para sistema operacional, quarentena local, logs e relatórios, com SSD integrado de aproximadamente, no mínimo, 240 GB.

3.1.29. Possuir no mínimo 8 (oito) interfaces de rede 1000Base-TX; Possuir no mínimo 12 (doze) interfaces 10GbE SFP+ integradas; 10.2.2.12.Possuir no mínimo 2 (duas) interfaces 10GbE SFP+;

3.1.30. Possuir no mínimo 1 slot de expansão para adição de módulos de interfaces de rede;

3.1.31. Deve ser compatível com módulos do mesmo fabricante com as seguintes opções:

3.1.32. 8 port GbE copper;

3.1.33. 8 port GbE SFP fiber;

3.1.34. 4 port 10 GbE SFP+ fiber;

3.1.35. 4 port GbE copper bypass (2 pairs);

3.1.36. 2 port 40 GbE QSFP+ fiber;

3.1.37. Deve suportar até 20 (vinte) interfaces em sua capacidade máxima de expansão usando os módulos do mesmo fabricante;

3.1.38. Possuir 1 (uma) interface do tipo console RJ-45ou similar.

3.1.39. Possuir fonte de alimentação 100–240 VAC autorreajustável.

3.1.40. Características Gerais para Firewall de Próxima Geração Tipo 1

3.1.41. Solução deve consistir de appliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW), e console de gerência, monitoração e logs.

3.1.42. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões.

3.1.43. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação.

3.1.44. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7.

3.1.45. O software deverá ser fornecido em sua versão mais atualizada.

3.1.46. O HA (modo de alta disponibilidade) deve suportar o uso de dois equipamentos em modo ativo-passivo ou modo ativo-ativo e deve possibilitar monitoração de falha de link.

3.1.47. Uma interface completa de comando de linha (CLI command-line-interface) deverá ser acessível através da interface gráfica e via porta serial.

3.1.48. A atualização de software deverá enviar avisos de atualização automáticos.

3.1.49. O sistema de objetos deverá permitir a definição de redes, serviços, hosts períodos de tempos, usuários e grupos, clientes e servidores.

3.1.50. O backup e o reestabelecimento de configuração deverão ser feitos localmente, via FTP ou email com frequência diária, semanal ou mensal, podendo também ser realizado por demanda.

3.1.51. As notificações deverão ser realizadas via email e SNMP.

3.1.52. Suportar SNMPv3 e Netflow.

3.1.53. O firewall deverá ser stateful, com inspeção profunda de pacotes.

3.1.54. As zonas deverão ser divididas pelo menos em WAN, LAN e DMZ, sendo necessário que as zonas LAN e DMZ possam ser customizáveis.

3.1.55. As políticas de NAT deverão ser customizáveis para cada regra.

3.1.56. A proteção contra flood deverá ter proteção contra DoS (Denial of Service), DdoS (Distributed DoS).

3.1.57. Proteção contra anti-spoofing.

3.1.58. Suportar IPv4 e IPv6.

3.1.59. Possuir certificação IPv6 Ready;

3.1.60. IPv6 deve suportar os tunelamentos 6in4, 6to4, 4in6 e IPv6 Rapid Deployment (6rd) de acordo com a RFC 5969.

3.1.61. Suportar NAT64 e NAT66 minimamente;

3.1.62. Suporte aos roteamentos estáticos, dinâmico (RIP, BGP e OSPF, OSPFv3) e multicast (PIM-SM e IGMP).

3.1.63. Deve suportar Roteamento BGP com uso de IPv6;

3.1.64. Suportar Delegação de Prefixo IPV6 (DHCP PD);

3.1.65. O firewall deve possuir integração com a plataforma de ZTNA do mesmo fabricante ou integrar de terceiros;

3.1.66. Deve possuir tecnologia de conectividade SD-WAN;

3.1.67. A funcionalidade SD-WAN deve suportar conectividade com o Secure SD-WAN oferecido no serviço Microsoft Azure Virtual WAN;

3.1.68. Deve suportar perfis de SD-WAN para balancear a carga das conexões entre as interfaces,

3.1.69. Deve possuir métodos de balanceamento: round-robin e persistência de sessão com as seguintes opções:

3.1.70. Os links podem ser ponderados para determinar como o tráfego é distribuído entre eles, podendo usar o SLA para selecionar quais links serão incluídos no balanceamento de carga. Conexão:

3.1.71. IP de origem; 10.2.3.28.2. IP de destino; 10.2.3.28.3. IP de origem e destino.

3.1.72. Deve suportar a configuração de nível mínimo de qualidade (latência, jitter e perda de pacotes) para que determinado link seja escolhido pelo SDWAN;

3.1.73. Deve suportar o uso de, no mínimo, 3 (três) links;

3.1.74. Deve suportar o uso de links de interfaces físicas, sub-interfaces lógicas de VLAN e túneis IPSec;

3.1.75. Deve gerar log de eventos que registrem alterações no estado dos links do SD-WAN, monitorados pela checagem de saúde;

3.1.76. A solução deverá ser capaz de medir o status de saúde do link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss, onde seja possível configurar um valor de Theshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN;

3.1.77. A solução de SD-WAN deve ser capaz de apresentar de forma gráfica, todos os dados de análise da saúde dos links, contendo gráficos que apresentam no mínimo os critérios descritos acima;

3.1.78. Os gráficos devem ser apresentados em tempo real e possibilitar a visualização histórica de pelo menos 24 horas, 48 horas, 1 semana e 1 mês; 10.2.3.36.A checagem de estado de saúde deve suportar a marcação de pacotes com DSCP, para avaliação mais precisa de links que possuem QoS configurado;
A solução deve possuir funcionalidade de criação da malha SD-WAN em diversos firewalls em um único concentrador;

3.1.79. Esta funcionalidade deve facilitar a configuração do SD-WAN de múltiplos firewalls, criando automaticamente todas as informações necessárias para que o SD-WAN aconteça, como pelo menos, mas não se limitando a: criação de rotas, regras de firewall, objetos e túneis VPNs necessárias;

3.1.80. A mesma console do concentrador de SD-WAN deve monitorar os links de cada dispositivo implementado, garantindo uma visualização única de todos os dispositivos implementados;

3.1.81. Deve possibilitar o roteamento baseado em VPNs;

3.1.82. Deve suportar criar políticas de roteamento;

3.1.83. Para as políticas de roteamento, devem ser permitidas pelo menos as seguintes condições

3.1.84. Interface de entrada do pacote;

3.1.85. IPs de origem;

3.1.86. IPs de destino;

3.1.87. Portas de destino;

3.1.88. Usuários ou grupos de usuários;

3.1.89. Aplicação em camada 7

3.1.90. Deve ser possível escolher um gateway primário e um gateway de backup para as políticas de roteamento

3.1.91. Deve suportar a definição de VLANs no firewall conforme padrão IEEE 802.1q e tagging de VLAN.

3.1.92. O balanceamento de link WAN deve permitir múltiplas conexões de links Internet, checagem automática do estado de links, failover automático e balanceamento por peso.

3.1.93. A solução deverá permitir port-aggregation de interfaces de firewall suportando o protocolo 802.3ad, para escolhas entre aumento de throughput e alta disponibilidade de interfaces;

3.1.94. Deve permitir a configuração de jumbo frames nas interfaces de rede;

3.1.95. Deve permitir a criação de um grupo de portas layer2;

3.1.96. A Solução física deverá apresentar compatibilidade com modens USB (3G/4G), onde apenas seja acionado na eventualidade de falha no link principal;

3.1.97. A solução deverá permitir configurar os serviços de DNS, Dynamic DNS, DHCP e NTP;

3.1.98. O traffic shapping (QoS) deverá ser baseado em rede ou usuário.

3.1.99. A solução deve permitir o tráfego de cotas baseados por usuários para upload/download e pelo tráfego total, sendo cíclicas ou não-cíclicas.

3.1.100. Deve possuir otimização em tempo real de voz sobre IP.

3.1.101. Deve implementar o protocolo de negociação Link Aggregation Control Protocol (LACP).

3.1.102. Controle por Políticas de Firewall

3.1.103. Deve suportar controles por: porta e protocolos TCP/UDP, origem/destino e identificação de usuários.

3.1.104. O controle de políticas deverá monitorar as políticas de redes, usuários, grupos e tempo, bem como identificar as regras não-utilizadas, desabilitadas, modificadas e novas políticas.

3.1.105. As políticas deverão ter controle de tempo de acesso por usuário e grupo, sendo aplicadas por zonas, redes e por tipos de serviços.

3.1.106. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança.

3.1.107. Controle de políticas por países via localização por IP.

3.1.108. Suporte a objetos e regras IPv6.

3.1.109. Suporte a objetos e regras multicast.

3.1.110. Prevenção de Ameaças

3.1.111. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus, Anti-Malware e Firewall de Proteção Web (WAF) integrados no próprio appliance de Firewall ou entregue em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação.

3.1.112. Deve realizar a inspeção profunda de pacotes para prevenção de intrusão (IPS) e deve incluir assinaturas de prevenção de intrusão (IPS).

3.1.113. As assinaturas de prevenção de intrusão (IPS) devem ser customizadas.

3.1.114. Deve possuir proteção de DNS, inclusa no licenciamento para fornecer um serviço de resolução de DNS seguro disponível globalmente com relatórios e controles de política integrados a console de gerenciamento centralizado.

3.1.115. Deve suportar o recebimento de feeds de ameaças de terceiros (IoC) minimamente com os seguintes formatos e autenticações: IP, dominio, URL, sem autenticação, autenticação de usuário e senha e via chave de API, sendo compatível com bases como: CrowdSec, GreyNoise, Cisco Talos, GitHub, TOR;

3.1.116. Entende-se que feeds de ameaças são uma lista de endereços IP, domínios e URLs envolvidos em atividades de ameaças, como phishing e malware. Esses objetos são chamados de Indicadores de Comprometimento (IoCs) ou indicadores de ataque.

3.1.117. Em appliances exclusivamente deve dispor de camada de proteção contra ameaças analizando os fluxos de tráfego usando o NDR ML(Network Detect and Response com Machine Learning) em nuvem, realizando análise de carga útil criptografada sem a necessidade de descriptografia TLS.

3.1.118. Exceções por usuário, grupo de usuários, IP de origem ou de destino devem ser possíveis nas regras;

3.1.119. Deve suportar granularidade nas políticas de IPS Antivírus e Anti-Malware, possibilitando a criação de diferentes políticas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens, com customização completa;

3.1.120. A solução contratada deve realizar a emulação de malwares desconhecidos em ambientes de sandbox em nuvem;

3.1.121. Para a eficácia da análise de malwares Zero-Day, a solução de Sandbox deve possuir algoritmos de inteligência artificial, como algoritmos baseados em machine learning ;

3.1.122. A funcionalidade de sandbox deve atuar como uma camada adicional ao motor de antimalware, e ao fim da análise do artefato, deverá gerar um relatório contendo oresultado da análise, bem como os screenshots das telas dos sistemas emulados pela plataforma;

3.1.123. Deve permitir configuração da exclusão de tipos de arquivos para que não sejam enviados para o sandbox em nuvem;

3.1.124. A proteção Anti-Malware deverá bloquear todas as formas de vírus, web malwares, trojans e spyware em HTTP e HTTPS, FTP e web-emails.

3.1.125. A proteção Anti-Malware deverá realizar a proteção com emulação JavaScript.

3.1.126. Deve ter proteção em tempo real contra novas ameaças criadas.

3.1.127. Deve possuir pelo menos duas engines de anti-vírus independentes e de diferentes fabricantes para a detecção de malware, podendo ser configuradas isoladamente ou simultaneamente.

3.1.128. Deve permitir o bloqueio de vulnerabilidades.

3.1.129. Deve permitir o bloqueio de exploits conhecidos.

3.1.130. Deve detectar e bloquear o tráfego de rede que busque acesso a command and control e servidores de controle utilizando múltiplas camadas de DNS, AFC e firewall.

3.1.131. Deve incluir proteção contra ataques de negação de serviços.

3.1.132. Ser imune e capaz de impedir ataques básicos como: SYN flood, ICMP flood, UDP Flood, etc.

3.1.133. Suportar bloqueio de arquivos por tipo.

3.1.134. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo.

3.1.135. Os eventos devem identificar o país de onde partiu a ameaça.

3.1.136. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas de segurança considerando uma das opções ou a combinação de todas elas: usuários, grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por usuários, grupos de usuários, origem, destino, zonas de segurança.

3.1.137. O filtro de email deve quarentenar os emails suspeitos ou realmente maliciosos;

3.1.138. A solução deve possibilitar aos usuários acessarem um painel para verificação da sua caixa pessoal de quarentena, possibilitando então a liberação ou a exclusão das mensagens;

3.1.139. A função de antispam deve permitir a configuração de relays com a possibilidade de autenticação dos mesmos;

3.1.140. A função de antispam deve possibilitar também o envio de emails seguros, realizando a criptografia das mensagens bem como dos seus anexos.

3.1.141. Deverá permitir a identificação dos IPs de origem através de proxy via "X-forward headers".

3.1.142. Deve possuir pelo menos duas engines de anti-vírus independentes e de diferentes fabricantes para a proteção da aplicação Web, podendo ser configuradas isoladamente ou simultaneamente.

3.1.143. Proteção pelo menos contra os seguintes ataques, mas não limitado a: SQL injection e Cross-site scripting.

3.1.144. Controle e Proteção de Aplicações

3.1.145. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações por assinaturas e camada 7, utilizando portas padrões (80 e 443), portas não padrões, port hopping e túnel através de tráfego SSL encriptado.

3.1.146. Deve ser possível inspecionar os pacotes criptografados com os algoritmos SSL 2.0, SSL 3.0, TLS 1.2 e TLS 1.3

3.1.147. O motor de análise de tráfego criptografado deve reconhecer, mas não limitado a, pelo menos os seguintes algorítimos: curvas elipticas (ECDH, ECDHE, ECDSA), DH, DHE, Authentication, RSA, DSA, ANON, Bulk ciphers, RC4, 3DES, IDEA, AES128, AES256, Camellia, ChaCha20-Poly1305, GCM, CCM, CBC, MD5, SHA1, SHA256, SHA384.

3.1.148. O motor de inspeção dos pacotes criptografados deve ser configurável e permitir definir ações como não decriptografar, negar o pacote e criptografar para determinadas conexões criptografadas

3.1.149. Reconhecer pelo menos 3.740 aplicações diferentes, classificadas por nível de risco, características e tecnologia, incluindo, mas não limitado a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, IA Generativa, update de software, serviços de rede, VoIP, streaming de mídia, proxy e tunelamento, mensageiros instantâneos, compartilhamento de arquivos, web e-mail e update de softwares.

3.1.150. Reconhecer pelo menos as seguintes aplicações: 4Shared File Transfer, Active Directory/SMB, Citrix ICA, DHCP Protocol, Dropbox Download, Easy Proxy, Facebook Graph API, Firefox Update, Freegate Proxy, FreeVPN Proxy, Gmail Video, Chat Streaming, Gmail WebChat, Gmail WebMail, Gmail-Way2SMS WebMail, Gtalk Messenger, Gtalk Messenger File Transfer, Gtalk-Way2SMS, HTTP Tunnel Proxy, HTTPort Proxy, LogMeIn Remote Access, NTP, Oracle database, RAR File Download, Redtube Streaming, RPC over HTTP Proxy, Skydrive, Skype, Skype Services, skyZIP, SNMP Trap, TeamViewer Conferencing e File Transfer, TOR Proxy, Torrent Clients P2P, Ultrasurf Proxy, UltraVPN, VNC Remote Access, VNC Web Remote Access, WhatsApp, WhatsApp File Transfer e WhatsApp Web.

3.1.151. Deve realizar o escaneamento e controle de micro app incluindo, mas não limitado a: Facebook (Applications, Chat, Commenting, Events, Games, Like Plugin, Message, Pics Download e Upload, Plugin, Post Attachment, Posting, Questions, Status Update, Video Chat, Video Playback, Video Upload, Website), Freegate Proxy, Gmail (Android Application, Attachment), Google Drive (Base, File Download, File Upload), Google Earth Application, Google Plus, LinkedIN (Company Search, Compose Webmail, Job Search, Mail Inbox, Status Update), SkyDrive File Upload e Download, Twitter (Message, Status Update, Upload, Website), Yahoo (WebMail, WebMail File Attach) e Youtube (Video Search, Video Streaming, Upload, Website)

3.1.152. Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante.

3.1.153. Atualizar a base de assinaturas de aplicações automaticamente.

3.1.154. Reconhecer aplicações em IPv6.

3.1.155. Limitar a banda usada por aplicações (traffic shaping).

3.1.156. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory e Azure AD, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários.

3.1.157. Deve ser possível adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras.

3.1.158. Deve permitir o uso individual de diferentes aplicativos para usuários que pertencem ao mesmo grupo de usuários, sem que seja necessária a mudança de grupo ou a criação de um novo grupo. Os demais usuários deste mesmo grupo que não possuírem acesso a estes aplicativos devem ter a utilização bloqueada.

3.1.159. Controle e Proteção Web

3.1.160. Deve permitir especificar política de navegação Web por tempo, ou seja, a definição de regras para um determinado dia da semana e horário de início e fim, permitindo a adição de múltiplos dias e horários na mesma definição de política por tempo. Esta regra de tempo pode ser recorrente ou em uma única vez.

3.1.161. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs e redes;

3.1.162. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via LDAP, Active Directory, Azure AD, Radius, E-directory e base de dados local;

3.1.163. Deve permitir autenticação em 2 fatores em conjunto com a autenticação Radius;

3.1.164. Permitir popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório;

3.1.165. Possuir pelo menos 90 categorias de URLs;

3.1.166. Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;

3.1.167. Deve ser capaz de forçar o uso da opção Safe Search em sites de busca;

3.1.168. Deve ser capaz de forçar as restrições do Youtube

3.1.169. Deve ser capaz de categorizar as URLs a partir de base ou cache de URLs locais ou através de consultas dinâmicas na nuvem do fabricante, independentemente do método de classificação a categorização não deve causar atraso na comunicação visível ao usuário;

3.1.170. Suportar a criação categorias de URLs customizadas;

3.1.171. Suportar a opção de bloqueio de categoria HTTP e liberação da categoria apenas em HTTPS.

3.1.172. Deve ser possível reconhecer o pacote HTTP independentemente de qual porta esteja sendo utilizada

3.1.173. Suportar a inclusão nos logs do produto de informações das atividades dos usuários;

3.1.174. Deve salvar nos logs as informações adequadas para geração de relatórios indicando usuário, tempo de acesso, bytes trafegados e site acessado.

3.1.175. Deve permitir realizar análise flow dos pacotes, entendendo exatamente o que aconteceu com o pacote em cada checagem;

3.1.176. Deve ser possível realizar caching do conteúdo web;

3.1.177. Deve realizar filtragem por mime-type, extensão e tipos de conteúdo ativos, tais como, mas não limitado a: ActiveX, applets e cookies.

3.1.178. Deve ser possível realizar a liberação de cotas de navegação para os usuários, permitindo que os usuários tenham tempos pré determinados para acessar sites na internet.

3.1.179. A console de gerenciamento deve possibilitar a visualização do tempo restante para cada usuário, bem como reiniciar o tempo restante com o intuito de zerar o contador.

3.1.180. Deve possuir capacidade de alguns usuários préviamente selecionados realizarem um bypass temporário na política de bloqueio atual.

3.1.181. A solução deve permitir o enforce dos domínios do Google e Office365 a fim de determinar em quais domínios os usuários poderão se autenticar;

3.1.182. Identificação de Usuários

3.1.183. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticando via LDAP, Active Directory, Azure AD, Radius, eDirectory, TACACS+ e via base de dados local, para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários.

3.1.184. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal).

3.1.185. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços.

3.1.186. Deve permitir autenticação em modos: transparente, autenticação proxy (explicito, NTLM e Kerberos) e autenticação via clientes nas estações com os sistemas operacionais Windows, macOS e Linux 32/64.

3.1.187. Ao se utilizar da opção de proxy explicito, deve permitir a autenticação por cada conexão, a fim de garantir que usuários logados em servidores de multisessão sejam identificados corretamente pelo firewall, mesmo quando utilizando-se apenas 1 IP de origem;

3.1.188. Deve possuir a autenticação Single sign-on para, pelo menos, os sistemas de diretórios Active Directory, Azure AD e eDirectory.

3.1.189. Dever suportar a configuração de logon único (Single sign-on) para que os administradores façam logon no console da Web usando o Azure AD

3.1.190. Deve suportar SSO do Azure AD para o Captive Portal;

3.1.191. Deve possuir um portal de acesso seguro a configurações e agente de VPN

3.1.192. Deve ser compatível com SSO Entra ID (Azure AD) para o agente de VPN client to site IPsec, SSL e o Portal de VPN

3.1.193. Deve possuir portal do usuário para que os usuários tenham acesso ao uso de internet pessoal, troquem senhas da base local e façam o download de softwares para as estações presentes na solução.

3.1.194. Qualidade de Serviço – QoS

3.1.195. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações.

3.1.196. A solução deverá suportar Traffic Shaping (Qos) e a criação de políticas baseadas em categoria web e aplicação por: endereço de origem; endereço de destino; usuário e grupo do LDAP/AD.

3.1.197. Deve ser configurado o limite e a garantia de upload/download, bem como ser priorizado o tráfego total e bitrate de modo individual ou compartilhado.

3.1.198. Suportar priorização Real-Time de protocolos de voz (VoIP).

3.1.199. Deve permitir aplicar prioridade mesmo após o roteamento, utilizando o protocolo DSCP;

3.1.200. Redes Virtuais Privadas – VPN

3.1.201. Suportar VPN Site-to-Site e Cliente-to-Site.

3.1.202. Suportar IPsec VPN.

3.1.203. Suportar SSL VPN.

3.1.204. Suportar L2TP e PPTP.

3.1.205. Suportar acesso remoto SSL, IPSec e VPN Client para Android e iPhone/iPAD.

3.1.206. Deve ser disponibilizado o acesso remoto ilimitado, até o limite suportado de túneis VPN pelo equipamento, sem a necessidade de aquisição de novas licenças e sem qualquer custo adicional para o licenciamento de clientes SSL.

3.1.207. Deve possuir o acesso via o portal de usuário para o download e configuração do cliente SSL para Windows.

3.1.208. Deve possuir opção de VPN IPSEC com client nativo do fabricante.

3.1.209. Deve possuir um portal encriptado baseado em HTML5 para suporte pelo menos a: RDP, SSH, Telnet e VNC, sem a necessidade de instalação de clientes VPN nas estações de acesso.

3.1.210. A VPN IPsec deve suportar: DES, 3DES, GCM, Suite-B, Autenticação MD5 e SHA-1;Diffie-Hellman Group 1, Group 2, Group 5 e Group 14; Algoritmo Internet Key Exchange (IKE); AES 128, 192 e 256 (Advanced Encryption Standard); SHA 256, 384 e 512; Autenticação via certificado PKI (X.509) e Pre-shared key (PSK).

3.1.211. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, SonicWALL, Fortinet, Huawei, Juniper, Palo Alto Networks e Sophos.

3.1.212. Deve suportar nativamente a integração com a Amazon, a fim de estabelecer um túnel seguro entre os appliances e o VPN da AWS.

3.1.213. Deve permitir criar políticas de controle de aplicações, IPS, Antivírus, Anti-Malware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;

3.1.214. Suportar autenticação via AD/LDAP, Token e base de usuários local;

3.1.215. Permitir estabelecer um túnel SSL VPN com uma solução de autenticação via LDAP, Active Directory, Azure AD, Radius, eDirectory, TACACS+ e via base de dados local.

3.1.216. Gerência Administrativa Centralizada

3.1.217. Deve possuir solução de gerenciamento centralizado, possibilitando o gerenciamento de diversos equipamentos através de uma única console central, com administração de privilégios e funções.

3.1.218. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança.

3.1.219. Estar licenciada para gerenciar as soluções de firewall de próxima geração Tipo1.

3.1.220. Devem ser fornecidas soluções virtuais ou via appliances desde que obedeçam a todos os requisitos desta especificação.

3.1.221. Deve ser centralizada a gerência de todas as políticas do firewall e configurações para as soluções de firewall de próxima geração Tipo1, sem necessidade de acesso direto aos equipamentos.

3.1.222. Deve permitir a criação de Templates para configurações.

3.1.223. Deve possuir indicadores do estado de equipamentos e rede.

3.1.224. Deve emitir alertas baseados em thresholds customizáveis, incluindo também alertas de expiração de subscrição, mudança de status de gateways, uso excessivo de disco, eventos ATP, IPS, ameaças de vírus, navegação, entre outros.

3.1.225. Deve permitir a criação de grupos de equipamentos por nome, modelo, firmware e regiões.

3.1.226. Deve ter controle de privilégios administrativos, com granularidade de funções (VPN admin, App e Web admin, IPS admin, etc);

3.1.227. Deve ter controle das alterações feitas por usuários administrativos, comparar diferentes versões de configurações e realizar o processo de roll back de configurações para mudanças indesejadas;

3.1.228. Deve ter logs de auditoria de uso administrativo e atividades realizadas nos equipamentos.

3.1.229. Deve ter integração com a solução de logs e relatórios, habilitando o provisionamento automatico de novos equipamentos e a sincronização dos administradores da centralização da gerência com a centralização de logs e relatórios.

3.1.230. Deve possibilitar o envio dos logs via syslog com conexão segura (TLS)

3.1.231. Gerência de Logs e Relatórios centralizados

3.1.232. Deve possuir solução de logs e relatórios centralizados, possibilitando a consolidação total de todas as atividades da solução através de uma única console central.

3.1.233. Estar licenciada para gerenciar as soluções de firewall de próxima geração Tipo1.

3.1.234. Deverá prover relatórios baseados em usuários,com visibilidade sobre acesso a aplicações, navegação, eventos ATP, downloads e consumo de banda, independente em qual rede ou IP o usuário esteja se conectando.

3.1.235. Deve possibilitar a identificação de ataques como a identificação de malware identificados pelos eventos ATP, usuários suspeitos, tráfegos anômalos incluindo tráfego ICMP e consumo não-usual de banda.

3.1.236. Deve conter relatórios pré-configurados, pelo menos de: aplicações, navegação, web server (WAF), IPS, ATP e VPN;

3.1.237. Deve fornecer relatórios históricos para análises de mudanças e comportamentos.

3.1.238. Deve conter customizações dos relatórios para inserção de logotipos próprios.

3.1.239. Deve fornecer relatórios de compliance SOX, HIPAA, GLBA, FISMA, PCI, CIPA

3.1.240. Deve permitir a exportação via PDF ou Excel.

3.1.241. Deve fornecer relatórios sobre os acessos de procura no Google, Yahoo, Bing e Wikipedia.

3.1.242. Deve fornecer relatórios de tendências.

3.1.243. Deve fornecer logs em tempo real, de auditoria e arquivados.

3.1.244. Deve possuir mecanismo de procura de logs arquivados.

3.1.245. Deve ter acesso baseado em Web com controles administrativos distintos.

3.1.246. Integração com Solução Endpoint

3.1.247. A solução de firewall deve possibilitar a integração com a solução de Endpoint (Sophos Cloud) instalada no ambiente da contratante;

3.1.248. A integração deve possibilitar a criação de regras de bloqueio de endpoints, com determinado status, dentro do Firewall de forma automática, sem que haja intervenção por parte do time da contratante.

3.1.249. A integração deverá ser nativa entre o firewall e o endpoint, ou

3.1.250. Utilizando APIs de integração da solução de firewall

3.1.251. Caso a integração não seja nativa, cabe a CONTRATADA:

3.1.252. Desenvolver completamente a solução de integração do Firewall e o Endpoint instalado (Sophos Cloud);

3.1.253. O Software de integração deve realizar a criação das regras do Firewall com no máximo 2 (dois) minutos após o incidente detectado no Endpoint;

3.1.254. Possuir interface WEB, acessada por HTTP ou HTTPS, para definição dos objetos das regras a serem criados, com no mínimo origem, destino, status do endpoint e protocolos;

3.1.255. Possibilitar o envio de emails sobre as ações do software;

3.1.256. Entregar o software de integração em máquina virtual, Windows ou Linux, juntamente com as devidas licenças necessárias para sistemas operacionais, banco de dados, etc;

3.1.257. A máquina virtual será instada no ambiente da contratante, não sendo permitido soluções em núvem;

3.1.258. A máquina virtual não deverá ter qualquer acesso remoto que não seja acordado pela contratante;

3.1.259. A mesma não deverá enviar/receber pacotes TCP/UDP ou por qualquer outro meio de comunicação, que não sejam os objetos de Firewall deste edital ou a console do endpoint da contratante;

3.1.260. A gestão do sistema operacional da máquina virtual em questão será de inteira responsabilidade da contratante, de modo a garantir que sejam realizados todos os updates, correções de patchs, segurança do sistema operacional, bem como com seus softwares, alterações de versões, etc.

3.1.261. A máquina virtual deve ser utilizada única e exclusivamente para o fim proposto no edital, não sendo permitido que a máquina virtual realize qualquer outra função;

3.1.262. Permitir backup das configurações do software de integração, possibiltando o restore em outra máquina virtual de forma a não comprometer o ambiente;

3.1.263. Realizar manutenção/alteração total no software de integração, sem custo adicional, durante o período de vigência do suporte do Firewall Tipo 1;

3.1.264. Realizar teste de bancada, a fim de comprovar a efetividade da integração;

3.1.265. Possuir atendimento 24 horas por dia, 07 dias por semana (24x7), durante todos os dias do ano, inclusive feriados;

3.1.266. O atendimento deve ser realizado por telefone, e-email, remoto ou on- site (ilimitado)

3.1.267. Apresentar SLA em contrato com os seguintes tempos:

3.1.268. Criticidade Baixa – Tempo de resposta de até 6 horas e até 48 horas para tempo de solução. Os casos definidos com criticidade baixa são: Falha na console de acesso Web do software de integração, alterações no funcionamento da ferramenta mediante solicitação da contratada, falhas no envio de emails por parte do software de integração.

3.1.269. Criticidade Média - Tempo de resposta de 4 horas e até 8 horas para tempo de solução. Os casos definidos com criticidade média são: Bloqueios inesperados realizados pelo software de integração, falha na identificação do status dos endpoints, falha no job de backup.

3.1.270. Criticidade Alta – Tempo de resposta de até 2 horas e até 6 horas para tempo de solução. Os casos definidos com criticidade alta são: Sistema operacional da máquina virtual do software de integração inoperante, com problemas durante o boot da VM, qualquer falha no software que comprometa o funcionamento da solução como um todo.

3.1.271. Integração com Plataformas de MDR

3.1.272. A solução deve ser capaz de integração com o serviço de MDR (Management dection and Response) do mesmo fabricante

3.1.273. A solução deve minimamente estar em roadmap com dois fabricantes proporcionando integração com plataformas de terceiros para recebimento de feeds de ameaças, cuja necessidade é o firewall usar para bloquear automaticamente o tráfego relacionado a ameaças.

3.1.274. A solução deve minimamente receber dados de feeds de ameaças nos seguintes protocolos: HTTPS, STIX, FTP e HTTP.

3.1.275. Solução de Validação do Acesso Remoto Seguro

3.1.276. A solução de acesso remoto seguro (ZTNA) deve estar licenciada para 50 (cinquenta) usuários;

3.1.277. Todos os componentes que fazem parte da solução deverão ser fornecidos por um único fabricante. Não serão aceitas composições de produtos de fabricantes diferentes;

3.1.278. 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 fermentas para a monitoração e controle da proteção dos dispositivos;

3.1.279. 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;

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

3.1.281. A solução deve possuir relatórios gráficos sobre pelo menos, mas não limitado à: aplicações, usuários, recursos e gateways;

3.1.282. A solução deverá fornecer acesso remoto para dispositivos de propriedade da empresa e de dispositivos não pertencentes à organização (BYOD);

3.1.283. A solução deverá fornecer acesso remoto para as aplicações corporativas hospedadas pela organização;

3.1.284. As aplicações podem estar hospedadas tanto em Data Centers locais, quanto em nuvens públicas;

3.1.285. A solução do tipo ZTNA, Zero trust network access, deve possibilitar a proteção das aplicações corporativas utilizando-se dos conceitos de Zero Trust Network Access como definidos pelo Gartner;

3.1.286. Não serão aceitas soluções que se baseiam em tecnologias de VPN para o seu funcionamento;

3.1.287. A solução deverá prover a micro segmentação do ambiente computacional, provendo o acesso a aplicações específicas definidas pelo administrador da solução;

3.1.288. A solução deverá funcionar com agente único;

3.1.289. Os gateways de operação e controle de acesso devem suportar no mínimo VMware ESXi 6.5 Hyper-V, Amazon AWS e conectores do próprio fabricante;

3.1.290. A solução deve possuir integração com produto de XDR do mesmo fabricante, assim possibilitando melhor visibilidade dos eventos em uma única console;

3.1.291. Deve ser possível a criação de clusters de gateways com o objetivo de escalar e balancear a carga de conexões;

3.1.292. Para implementação do Gateway, deve possibilitar implementar utilizando no mínimo 4Gb de memória RAM;

3.1.293. A solução deverá prover a instalação de múltiplos gateways de operação sem custo adicional;

3.1.294. A solução deverá ser compatível com Microsoft Windows e macOS deve estar em Roadmap a integração com sistemas operacionais móveis, como Apple iOS e Android;

3.1.295. A solução deverá fornecer uma conexão segura de pré-autenticação antes da sequência de login para permitir o login "online" seguro para dispositivos Windows;

3.1.296. Deve possibilitar a integração com provedores de autenticação externos, suportando pelo menos, mas não limitado a: Microsoft Azure AD e OKTA Open ID;

3.1.297. A solução deverá possuir políticas de controle de acesso personalizáveis com base na identidade, critérios como grupos de usuários, aplicações e gateways de aplicativos.

3.1.298. A solução deverá ser capaz de operar em portas de protocolos não padrões da Internet (por exemplo, tcp/8081);

3.1.299. A solução deverá suportar também aplicações pré-determinadas contendo, pelo menos, mas não limitado a: HTTP/HTTPS, Remote Desktop Protocol (RDP) e Secure Shell (SSH);

3.1.300. A solução deverá suportar TLS 1.2 para conexões criptográficas;

3.1.300.1 A solução deverá ter comparabilidade futura com TLS 1.3; 10.2.15.27. A solução deve ser licenciada por usuário no qual se beneficiará da solução, não sendo obrigatoriamente necessário licenciar todos os usuários e/ou dispositivos existentes;

3.1.301. A solução deve permitir gestão centralizada de ZTNA, Firewall, Endpoints e outros produtos de segurança através de console unificado em nuvem.

3.1.302. O licenciamento deve contemplar gateways gratuitos e ilimitados para expansão sem custo adicional.

3.1.303. A solução deve integrar o conceito de Security Heartbeat para avaliar a integridade do dispositivo em tempo real.

3.1.304. A solução deve restringir o acesso a aplicações com base no status de integridade do dispositivo.

3.1.305. A solução deve suportar failover entre pontos de presença na nuvem com zero downtime.

3.1.306. A solução deve oferecer relatórios detalhados sobre o uso de aplicativos, tentativas de acesso e dispositivos conectados.

3.1.307. Deve suportar autenticação contínua e integração com múltiplos IDPs, incluindo Azure AD e Okta.

3.1.308. A solução deve permitir acesso clientless para aplicações web via navegador.

3.1.309. A solução deve fornecer agente único para proteção de endpoint e ZTNA.

3.1.310. A solução deve implementar microssegmentação para limitar acessos por aplicação e evitar movimento lateral na rede.

3.1.311. Deve integrar-se com soluções de autenticação multifator (MFA) para reforçar segurança na autenticação.

3.1.312. Deve ser compatível com sistemas Windows, macOS e acesso web via navegadores sem necessidade de cliente.

3.1.313. Deve oferecer logs completos para auditoria, conformidade e análise forense.

3.1.314. A solução deve suportar clusters de gateways para balanceamento de carga e alta disponibilidade.

3.1.315. Características Específicas de Desempenho Solução de Endpoint

3.1.316. Características Gerais da Solução

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

3.1.318. O escopo do projeto consiste em fornecimento de proteção para 320 (Trezentos e Vinte) Dispositivos, dentre eles, 20 (Vinte) Servidores.

3.1.319. 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 fermentas para a monitoração e controle da proteção dos dispositivos;

3.1.320. A console de nuvem deve possuir o armazenamento de seus dados dentro do território nacional, garantindo conformidade e compliance com as leis locais como a LGPD, Instrução normativa 5 e NC-14 determinada pelo Banco Central;

3.1.321. 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;

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

3.1.323. Deve possuir capacidade de realizar a integração com soluções de firewalls para criar políticas automáticas em caso de ataques em massa nos computadores e servidores;

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

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

3.1.326. Deve possuir a possibilidade de aplicar regras diferenciadas baseado em grupos ou usuários;

3.1.327. A instalação deve ser feita via cliente específico por download da gerência central ou também via email de configuração. O instalador deverá permitir a distribuição do cliente via Active Directory (AD) para múltiplas máquinas;

3.1.328. 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;

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

3.1.330. Deve permitir exclusões de escaneamento para um determinado websites, pastas, arquivos ou aplicações, tanto a nível geral quanto específico em uma determinada política.

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

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

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

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

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

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

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

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

3.1.339. 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;

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

3.1.341. Detalhar quais usuários estão ativos, inativos ou desprotegidos, bem como detalhes dos mesmos;

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

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

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

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

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

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

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

3.1.349. 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. Deve ser bloqueado o upload ou removida a informação confidencial antes do envio do arquivo;

3.1.350. As portas de comunicação deverão ser configuráveis. A comunicação deverá permitir QoS para controlar a largura de banda de rede.

3.1.351. A solução deverá permitir a seleção da versão do software de preferência, permitindo assim o teste da atualização sobre um grupo de PCs piloto antes de implantá-lo para toda a rede. Permitir ainda selecionar um grupo de computadores para aplicar a atualização para controlar a largura de banda de rede. A atualização da versão deverá ser transparente para os usuários finais.

3.1.352. O agente anti-vírus 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;

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

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

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

3.1.356. 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;

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

3.1.358. 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;

3.1.359. 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;

3.1.360. Deverá possuir interface gráfica web, com suporte a língua portuguesa (padrão brasileiro);

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

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

3.1.363. 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;

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

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

3.1.366. Forçar uma atualização naquele momento;

3.1.367. Ver os detalhes dos eventos ocorridos;

3.1.368. Executar verificação completa do sistema; 10.3.1.53.Forçar o cumprimento de uma nova política de segurança; 10.3.1.54.Mover o computador para outro grupo;

3.1.369. Apagar o computador da lista;

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

3.1.371. 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;

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

3.1.373. 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;

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

3.1.375. Nome do dispositivo;

3.1.376. Início da proteção;

3.1.377. Último usuário logado no dispositivo;

3.1.378. Último update;

3.1.379. Último escaneamento realizado;

3.1.380. Status de proteção do dispositivo;

3.1.381. Grupo a qual o dispositivo faz parte;

3.1.382. Permitir a execução manual de todos estes relatórios danos formatos CSV e PDF;

3.1.383. A console deve possuir métodos de verificação da saúde das configurações da console, possibilitando aos administradores descobrirem facilmente se existe alguma falha de configuração que pode facilitar a entrada de malwares e invasores no ambiente;

3.1.384. Características Gerais da Solução de Proteção para Estações de Trabalho

3.1.385. Características básicas do agente de proteção contra malwares

3.1.386. Pré-execução do agente para verificar o comportamento malicioso e detectar malware desconhecido;

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

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

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

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

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

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

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

3.1.394. 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;

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

3.1.396. 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);

3.1.397. Suportar máquinas com arquitetura 32-bits e 64-bits (Exceto para Windows 11 que não há opção de 32bits;

3.1.398. O cliente para instalação em estações de trabalho deverá ser compatível com os sistemas operacionais, macOS 13 Ventura, macOS 14 Sonoma, macOS 15 Sequoia, macOS 26 (Tahoe), Microsoft Windows 7, 8.1, 10 e 11;

3.1.399. Para macOS a solução deve ser compatível com a execução nativa em processadores Apple Silicon, não serão aceitas soluções que dependem de emulação via Rosetta2 da Apple.

3.1.400. 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;

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

3.1.402. Funcionalidade de Firewall e Detecção e Proteção de Intrusão (IDS\IPS) com as funcionalidades:

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

3.1.404. Capacidade de reconhecer e bloquear automaticamente as aplicações em clientes baseando-se na impressão digital (hash) do arquivo ou dinamicamente através do nome da aplicação;

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

3.1.406. 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.

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

3.1.408. Deve possuir técnicas de proteção, que inclui:

3.1.409. Análise dinâmica de código - técnica para detectar malware criptografado mais complexo;

3.1.410. Algorítimo correspondente padrão - onde os dados de entrada são comparados com um conjunto de sequências conhecidas de código já identificados como um vírus;

3.1.411. 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;

3.1.412. 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);

3.1.413. 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;

3.1.414. Características básicas do agente de proteção contra malwares

3.1.415. Funcionalidade de Antivírus e AntiSpyware:

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

3.1.417. 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.

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

3.1.419. 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;

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

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

3.1.422. 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;

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

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

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

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

3.1.427. Controle de acesso a sites por categoria;

3.1.428. 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.

3.1.429. 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;

3.1.430. 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;

3.1.431. Capacidade de verificar somente arquivos novos e alterados

3.1.432. Funcionalidades especificas 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.

3.1.433. Funcionalidade de detecção Pró-Ativa de reconhecimento de novas ameaças

3.1.434. Funcionalidade de detecção de ameaças via técnicas de machine learning;

3.1.435. Deve prover de funcionalidade avançada de proteção preditiva baseada em inteligência artificial e machine learning, capaz de ajustar automaticamente políticas de segurança com base em comportamentos suspeitos e ameaças emergentes, para que possa reduzir a superfície de ataque ao ativar controles adaptativos de acordo com o contexto do ambiente, sem a necessidade de intervenção manual constante.

3.1.436. A solução de proteção contra ameaças e demais recursos da solução devem funcionar em Modo de segurança do Windows;

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

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

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

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

3.1.441. Funcionalidade de proteção contra ransomwares:

3.1.442. Para estações de trabalho, dispor de capacidade de proteção contra ransomware não baseada exclusivamente na detecção por assinaturas; 10.4.2.2.10. Para estações de trabalho, dispor de capacidade de remediação da ação de criptografia maliciosa dos ransomwares;

3.1.443. A Solução deve ter a capacidade de reverter automaticamente arquivos afetados por ransomware durante a sua execução em tempo real, através de uma tecnologia proprietária sem depender de VSS (Volume Shadow Copy);

3.1.444. 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;

3.1.445. A solução deverá previnir ameaças e interromper que eles sejam executadas em dispositivos da rede, detectando e limpando os malwares, além da realização de uma análise detalhada das alterações realizadas.

3.1.446. Deve possuir uma tecnologia anti-exploit baseada em comportamento, reconhecendo e bloqueando as mais comuns técnicas de malware, protegendo os endpoints de ameaças desconhecidas e vulnerabilidades zero-day.

3.1.447. Deve ser realizada a detecção e o bloqueio de, pelo menos, as seguintes técnicas de exploit:

3.1.448. DEP (Data Execution Prevention);

3.1.449. Address Space Layout Randomization (ASLR);

3.1.450. Bottom Up ASLR;

3.1.451. Null Page;

3.1.452. Anti-HeapSpraying;

3.1.453. Dynamic Heap Spray;

3.1.454. Import Address Table Filtering (IAF);

3.1.455. VTable Hijacking; 10.4.2.2.24.

Stack Pivot and Stack Exec;

3.1.456. SEHOP;

3.1.457. Stack-based ROP (Return-Oriented Programming);

3.1.458. Control-Flow Integrity (CFI);

3.1.459. Syscall;

3.1.460. WOW64;

3.1.461. Load Library;

3.1.462. Shellcode;

3.1.463. VBScript God Mode;

3.1.464. Application Lockdown;

3.1.465. Process Protection;

3.1.466. Network Lockdown.

3.1.467. A solução deverá trabalhar silenciosamente na máquina do usuário e deverá detectar a criptografia maliciosa de dados (ransomware), realizando a sua interrup-

ção. No caso de arquivos serem criptografados a solução deverá realizar o retorno destes arquivos ao seu estado normal. Deste modo a solução deve ser capaz de fazer a limpeza e remoção completa do ransomware na máquina do usuário.

3.1.468. Deve fornecer também uma análise detalhada das modificações realizadas pelo ransomware, realizando a correlação dos dados em tempo real, indicando todas as modificações feitas em registros, chaves, arquivos alvos, conexões de redes e demais componentes contaminados.

3.1.469. A console de monitoração e configuração deverão ser feitas 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 para a solução de anti-exploit e anti-ransomware.

3.1.470. 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, bem como todas as identificações para o mapeamento instantâneo dos efeitos causados pelo ransomware nos endpoints.

3.1.471. Solução de Endpoint Detection and Response (EDR)

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

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

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

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

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

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

3.1.478. A solução e as detecções devem apresentar Táticas empregadas baseadas no MITRE ATT&CK

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

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

3.1.481. 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;

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

3.1.483. 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;

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

3.1.485. 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;

3.1.486. Deve ter acesso a recurso de Data Lake que armazene informações críticas de endpoints e servidores, permitindo o acesso aos dados sobre atividades mesmo-quando o dispositivo correspondente está offline ou foi descontinuado;

3.1.487. Deve possibilizar o agendamento de consultas (queries);

3.1.488. Deve reter os dados no Data Lake por no mínimo 90 dias.

3.1.489. Funcionalidade de Controle de Aplicações e Dispositivos

3.1.490. 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;

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

3.1.492. 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;

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

3.1.494. Proibir através de política a inicialização de um processo ou aplicativo baseado em nome ou no hash do arquivo;

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

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

3.1.497. 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;

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

3.1.499. 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;

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

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

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

3.1.503. Permitir que todos os dispositivos do mesmo modelo;

3.1.504. Permitir que um único dispositivo com base em seu número de identificação único;

3.1.505. Permitir o acesso total;

3.1.506. Permitir acesso somente leitura;

3.1.507. Permitir ainda o bloqueio de pontes entre duas redes, por exemplo, um laptop conectado ao mesmo tempo na LAN e se tornar um hotspot Wi-Fi, ou através de um modem.

3.1.508. Funcionalidade de Proteção e Prevenção e Perda de Dados 10.4.2.5.1.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;

3.1.509. 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);

3.1.510. 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;

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

3.1.512. Números de cartões de crédito; 10.4.2.5.6.Números de contas bancárias; 10.4.2.5.7.Números de Passaportes; 10.4.2.5.8.Endereços;

3.1.513. Números de telefone;

3.1.514. Códigos postais definidas por países como Brasil, França, Inglaterra, Alemanha, EUA, etc;

3.1.515. Lista de e-mails;

3.1.516. Informações pessoais, corporativas e financeiras referentes especificamente ao Brasil, como CPF, RG, CNH, CNPJ, dados bancários, etc;

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

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

3.1.519. 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;

3.1.520. Permitir o controle de dados para no mínimo os seguintes meios: 10.4.2.5.17. Anexado no cliente de e-mail (ao menos Outlook e Outlook Express); 10.4.2.5.18. Anexado no navegador (ao menos IE, Firefox e Chrome);

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

3.1.522. Anexado a dispositivos de armazenamento (ao menos USB, CD/DVD);

3.1.523. Características Gerais da Solução de Proteção para Servidores

3.1.524. Características Básicas do Agente da Proteção contra Malwares 10.4.3.1.1. 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;

3.1.525. Deve realizar a pré-execução do agente para verificar o comportamento malicioso e detectar malwares desconhecidos;

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

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

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

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

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

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

3.1.532. 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;

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

3.1.534. 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);

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

3.1.536. Windows Server 2008 R2;

3.1.537. Windows Server 2016;

3.1.538. Windows Server 2012 R2 (64 bits);

3.1.539. Windows Server 2012 (64 bits);

3.1.540. Amazon Linux;

3.1.541. Amazon Linux 2;

3.1.542. CentOS 7;

3.1.543. Debian 10;

3.1.544. Oracle Linux 7;

3.1.545. Oracle Linux 8;

3.1.546. Red Hat Enterprise 7;

3.1.547. Red Hat Enterprise 8;

3.1.548. Red Hat Enterprise 9;

3.1.549. SUSE Linux Enterprise Server 12;

3.1.550. SUSE Linux Enterprise Server 15;

3.1.551. Ubuntu 20.04 LTS;

3.1.552. Ubuntu 22.04 LTS;

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

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

3.1.555. 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;

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

3.1.557. Deve possuir funcionalidades de tecnologias conhecidas como CWPP – Cloud Workload Protection Plataform, permitindo que seja possível trazer funcionalidades de próxima geração para cargas de trabalho em nuvem, bem como containers, e afins;

3.1.558. A solução deve no mínimo, utilizar o modelo de sensores para containers, garantindo visibilidade e proteção de, no mínimo, estes tipos de ataques:

3.1.559. Escalação de privilégios dentro de containers;

3.1.560. Programas utilizando técnicas de mineração de criptomoedas;

3.1.561. Detecção de atacantes tentando destruir evidências de ambientes comprometidos (IOC – Indicator of compromise);

3.1.562. Detecção de funções internas do kernel que estão sendo adulteradas em um host;

3.1.563. A solução deve também se integrar a tecnologias de CSPM – Cloud Security Posture Management, tendo como objetivo trazer funcionalidades de análises integradas de CWPP e CSPM a fim de melhorar a visibilidade e resposta à incidentes em ambientes de nuvem públicas,

3.1.564. Funcionalidade de Firewall e Detecção e Proteção de Introdução (IDS/IPS) com as funcionalidades

3.1.565. Possuir proteção contra exploração de buffer overflow;

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

3.1.567. Deve prover de funcionalidade avançada de proteção preditiva baseada em inteligência artificial e machine learning, capaz de ajustar automaticamente políticas de segurança com base em comportamentos suspeitos e ameaças emergentes, para que possa

reduzir a superfície de ataque ao ativar controles adaptativos de acordo com o contexto do ambiente, sem a necessidade de intervenção manual constante.

3.1.568. A solução de proteção contra ameaças e demais recursos da solução devem funcionar em Modo de segurança do Windows;

3.1.569. Capacidade de reconhecer e bloquear automaticamente as aplicações em clientes baseando-se na impressão digital (hash) do arquivo ou dinamicamente através do nome da aplicação.

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

3.1.571. 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.

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

3.1.573. Deve possuir técnicas de proteção, que inclui:

3.1.574. Análise dinâmica de código - técnica para detectar malware criptografado mais complexo;

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

3.1.576. 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;

3.1.577. 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);

3.1.578. 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;

3.1.579. A solução e as detecções devem apresentar Táticas empregadas baseadas no MITRE ATT&CK

3.1.580. Funcionalidade de Antivírus e AntiSpyware

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

3.1.582. 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.

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

3.1.584. 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;

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

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

3.1.587. Capacidade de detectar arquivos através da reputação deles;

3.1.588. 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;

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

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

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

3.1.592. Proteger arquivos de documento contra-ataques do tipo ransomwares; 10.4.3.3.13. Proteger que o ataque de ransomware seja executado remotamente; 10.4.3.3.14. Permitir o envio de amostras de malwares para a nuvem de inteligência do fabricante;

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

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

3.1.595. Controle de acesso a sites por categoria;

3.1.596. 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.

3.1.597. 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;

3.1.598. 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;

3.1.599. Capacidade de verificar somente arquivos novos e alterados;

3.1.600. Funcionalidades especificas 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.

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

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

3.1.603. Funcionalidade de Proteção contra Ransomwares

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

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

3.1.606. 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;

3.1.607. A Solução deve ter a capacidade de reverter automaticamente arquivos afetados por ransomware durante a sua execução em tempo real, através de uma tecnologia proprietária, sem depender de VSS (Volume Shadow Copy);

3.1.608. Funcionalidade de Controle de Aplicações e Dispositivos

3.1.609. 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;

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

3.1.611. 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;

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

3.1.613. Proibir através de política a inicialização de um processo ou aplicativo baseado em nome ou no hash do arquivo;

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

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

3.1.616. 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;

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

3.1.618. 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;

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

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

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

3.1.622. Permitir que todos os dispositivos do mesmo modelo;

3.1.623. Permitir que um único dispositivo com base em seu número de identificação único;

3.1.624. Permitir o acesso total;

3.1.625. Permitir acesso somente leitura;

3.1.626. Permitir ainda o bloqueio de pontes entre duas redes, por exemplo, um laptop conectado ao mesmo tempo na LAN e se tornar um hotspot Wi-Fi, ou através de um modem.

3.1.627. Funcionalidade de Proteção e Prevenção a Perda de Dados

3.1.628. 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;

3.1.629. 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);

3.1.630. 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;

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

3.1.632. Números de cartões de crédito; 10.4.3.6.4.2. Números de contas bancárias; 10.4.3.6.4.3. Números de Passaportes; 10.4.3.6.4.4. Endereços;

3.1.633. Números de telefone;

3.1.634. Códigos postais definidas por países como Brasil, França, Inglaterra, Alemanha, EUA, etc;

3.1.635. Lista de e-mails;

3.1.636. Informações pessoais, corporativas e financeiras referentes especificamente ao Brasil, como CPF, RG, CNH, CNPJ, dados bancários etc.;

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

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

3.1.639. 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;

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

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

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

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

3.1.644. Anexado a dispositivos de armazenamento (ao menos USB, CD/DVD);

3.1.645. Solução de Endpoint Detection and Response (EDR)

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

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

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

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

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

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

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

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

3.1.654. 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;

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

3.1.656. 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;

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

3.1.658. 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;

3.1.659. Deve ter acesso a recurso de Data Lake que armazene informações críticas de endpoints e servidores, permitindo o acesso aos dados sobre atividades mesmo quando o dispositivo correspondente está offline ou foi descontinuado;

3.1.660. Deve possibilizar o agendamento de consultas;

3.1.661. Deve reter os dados no Data Lake por no mínimo 7 dias.

3.1.662. Dispositivos Ethernets Remotos

3.1.663. Deverá ser possível gerenciamento através de Cloud Sophos Central e On-premises for Sophos XG/XGS Firewall;

3.1.664. O equipamento deverá possuir capacidade mínima de taxa de transferência de túnel de 850 Mbps.

3.1.665. Deve contar com, no mínimo, 4 portas LAN 10/100/1000 Base-TX (Gigabit Ethernet);

3.1.666. No mínimo, 2 portas WAN 10/100/1000 Base-TX, sendo uma das portas WAN compartilhada com uma porta SFP;

3.1.667. Deve incluir ao menos 1 porta SFP (fibra óptica) compatível com interface WAN;

3.1.668. O equipamento deve oferecer, no mínimo, 2 portas com suporte a Power over Ethernet (PoE), com potência total de, no mínimo, 30 W.

3.1.669. Possuir, no mínimo, 2 portas USB 3.0 (uma frontal e uma traseira), além de uma porta Micro-USB para acesso via console.

3.1.670. Deve oferecer compartimento modular com suporte a conectividade opcional via Wi-Fi, com tecnologia 802.11ac (Wi-Fi 5) e ao menos 2 antenas MIMO.

3.1.671. Deve ser compatível com módulos de conectividade 3G/4G LTE utilizando cartões NMC7430/MC7455 Sierra Wireless.

3.1.672. A fonte de alimentação deve ter entrada de 110–240 VCA, 50–60 Hz, com saída de 12V ± 10%, 6.95A, 75W.

3.1.673. Deve fornecer suporte a fonte de alimentação redundante;

3.1.674. O consumo de energia deverá ser de até 11,8 W em modo de espera, até 25,33 W em operação plena sem PoE e até 62,48 W em operação plena com PoE.

3.1.675. As dimensões mínimas devem ser de 225 mm de largura, 44 mm de altura e 150 mm de profundidade.

3.1.676. O equipamento deve possuir certificações CE, FCC, IC, RCM, VCCI, CB, UL, CCC, KC e ANATEL.

3.1.677. O equipamento deverá ser compatível com solução SD-WAN de gerenciamento centralizado do fabricante, permitindo gerenciamento remoto, configuração central e atualizações de firmware automáticas.

3.1.678. O equipamento deverá permitir, gerenciamento centralizado via interface web ou sistema de gerenciamento em nuvem, atualizações automáticas de firmware, monitoramento de estado e logs de eventos e integração com sistemas de gerenciamento de rede do fabricante.

3.1.679. O equipamento deve utilizar comunicação criptografada entre os pontos, com suporte a criptografia de no mínimo AES 256 bits para túneis VPN e comunicação com a central.

3.1.680. Deverá ser acompanhado de licença, suporte e garantia mínima de 01 (um) ano;

3.1.681. O equipamento deve suportar configuração automática (plug-and-play), sem necessidade de configuração local por técnicos, utilizando a infraestrutura do fabricante para ativação e provisionamento remoto.

3.1.682. Caso necessário, poderá ser exigido do fornecedor apoio técnico na instalação e treinamento para a equipe de TI local, presencial ou remoto, sem custos adicionais.

3.1.683. Os equipamentos devem realizar a conexão via VPN de forma nativa e estar totalmente integrada com o firewall Sophos XG/XGS, contando com administração web através do Cloud Sophos Central. Deverá atender os requisitos para o fornecimento destes dispositivos Ethernet Remoto e garantir melhor desempenho de aplicativos e obter melhor visibilidade da integridade da rede para assegurar que as suas localidades remotas atinjam o mesmo desempenho que a administração principal escritório central.

3.1.684. Os documentos, manuais e softwares de instalação deverão ser fornecidos, sempre que possível, em língua portuguesa, ou, na sua impossibilidade, em língua inglesa.

3.1.685. O suporte aos componentes do serviço deve compreender o acesso a serviço de helpdesk para abertura/acompanhamento de chamados em língua portuguesa, incluindo o atendimento telefônico e o atendimento via e-mail ou sítio Web.

3.1.686. Os equipamentos devem possuir fonte de alimentação com bivolt automático e cabos de alimentação no padrão brasileiro de tomadas.

3.1.687. Deverá ser provida, por meio de um appliance físico ou virtual, uma solução de gerenciamento centralizado, possibilitando o gerenciamento dos equipamentos necessários aos serviços de Firewall, permitindo controle sobre todos os equipamentos da plataforma de segurança em uma única console, com administração de privilégios, funções e políticas para todos os equipamentos que compõe a plataforma de segurança.

3.1.688. Deverá ser realizada reunião inicial de alinhamento de expectativas logo após a assinatura do contrato, onde serão discutidos os serviços de preparação da infraestrutura básica de funcionamento, migração de dados e demais adequações necessárias à entrega da solução.

3.1.689. A solução deve ser capaz de atender às seguintes especificações mínimas dos serviços, a serem ofertados em uma única plataforma:

3.1.690. O portal de acompanhamento dos serviços deverá possibilitar que sejam visualizados e impressos relatórios das informações de desempenho a respeito dos ser-

viços prestados, ou seja, a CONTRATADA deverá fornecer acesso a relatórios e dashboards como forma de acompanhamento do contrato, para uso como ferramenta da fiscalização, para verificar se os serviços estão sendo prestados de acordo com o disposto neste Termo.

3.1.691. A CONTRATADA deverá conduzir as atividades utilizando o conhecimento da metodologia utilizada pelo fabricante, aplicando-as de acordo com o ambiente da CONTRATANTE e suas políticas de negócios, de forma a obter o melhor resultado tanto em performance quanto em segurança.

3.1.692. Deverá ser possível gerenciamento através de Cloud Sophos Central e On-premises for Sophos XG/XGS Firewall;

3.1.693. O equipamento deverá possuir capacidade mínima de taxa de transferência de túnel de 850 Mbps.

3.1.694. Deve contar com, no mínimo, 4 portas LAN 10/100/1000 Base-TX (Gigabit Ethernet), no mínimo, 2 portas WAN 10/100/1000 Base-TX, sendo uma das portas WAN compartilhada com uma porta SFP;

3.1.695. Deve incluir ao menos 1 porta SFP (fibra óptica) compatível com interface WAN;

3.1.696. O equipamento deve oferecer, no mínimo, 2 portas com suporte a Power over Ethernet (PoE), com potência total de, no mínimo, 30 W.

3.1.697. Possuir, no mínimo, 2 portas USB 3.0 (uma frontal e uma traseira), além de uma porta Micro-USB para acesso via console.

3.1.698. Deve oferecer compartimento modular com suporte a conectividade opcional via Wi-Fi, com tecnologia 802.11ac (Wi-Fi 5) e ao menos 2 antenas MIMO.

3.1.699. Deve ser compatível com módulos de conectividade 3G/4G LTE utilizando cartões MC7430/MC7455 Sierra Wireless.

3.1.700. A fonte de alimentação deve ter entrada de 110–240 VCA, 50–60 Hz, com saída de 12V ± 10%, 6.95A, 75W.

3.1.701. Deve fornecer suporte a fonte de alimentação redundante;

3.1.702. O consumo de energia deverá ser de até 11,8 W em modo de espera, até 25,33 W em operação plena sem PoE e até 62,48 W em operação plena com PoE.

3.1.703. As dimensões mínimas devem ser de 225 mm de largura, 44 mm de altura e 150 mm de profundidade.

3.1.704. O equipamento deve possuir certificações CE, FCC, IC, RCM, VCCI, CB, UL, CCC, KC e ANATEL.

3.1.705. O equipamento deverá ser compatível com solução SD-WAN de gerenciamento centralizado do fabricante, permitindo gerenciamento remoto, configuração central e atualizações de firmware automáticas.

3.1.706. O equipamento deverá permitir, gerenciamento centralizado via interface web ou sistema de gerenciamento em nuvem, atualizações automáticas de firmware, monitoramento de estado e logs de eventos e integração com sistemas de gerenciamento de rede do fabricante.

3.1.707. O equipamento deve utilizar comunicação criptografada entre os pontos, com suporte a criptografia de no mínimo AES 256 bits para túneis VPN e comunicação com a central.

3.1.708. Deverá ser acompanhado de licença, suporte e garantia mínima de 01 (um) ano;

3.1.709. O equipamento deve suportar configuração automática (plug-and-play), sem necessidade de configuração local por técnicos, utilizando a infraestrutura do fabricante para ativação e provisionamento remoto.

3.1.710. Caso necessário, poderá ser exigido do fornecedor apoio técnico na instalação e treinamento para a equipe de TI local, presencial ou remoto, sem custos adicionais.

3.1.711. Será necessário a contratação de um novo link de Internet além do link existente ou não que interliga a Rede Corporativa da Prefeitura. Em outras situações, os dois ou mais links poderão ser de Operadoras de Telecom sem passar por conex]ao a Rede Coirporativa da Prefeitura tornando o processo do link com a Internet de forma transparente a partir da utilização do Equipamento para Ethernet Remoto.

3.1.712. Execução

3.1.713. É responsabilidade da CONTRATADA definir projeto de implantação, com atividades, cronograma e dimensionamento de recursos, de forma a atender os requisitos de nível de serviço e prazos estabelecidos na Especificação dos Serviços.

3.1.714. A empresa CONTRATADA fornecerá um serviço de onboarding para a tecnologia onde trabalhará com o CONTRATANTE para integrar a solução e suportar a configuração e integração corretas das fontes, incluindo as seguintes:

3.1.715. A CONTRATADA fornecerá documentação arquitetónica que identifica os pontos de conexão entre a solução ofertada, o ambiente do CONTRATANTE e o ambiente de serviço.

3.1.716. A CONTRATADA coordenará todas as responsabilidades, tarefas e relatórios de status de CONTRATANTE relacionados à entrega do recurso, e orientará e ajudará CONTRATANTE na transição para co-gerenciar a Tecnologia Contratada.

3.1.717. A fase de onboarding deve seguir pelo menos 5 fases com os seguintes requisitos mínimos:

3.1.718. Kick-off call: Alinhamento de objetivos e expectativas, alinhamento do onboard e da jornada. Alinhamento das integrações e configurações necessárias. Defininição de próximos passos.

3.1.719. Serviço de Implementação e Configuração: Definição de melhores práticas de Configuração, configuração de Integração com as ferramentas definidas, Treinamento, implantação em ambiente e avaliação de postura de Segurança.

3.1.720. Workshop de demonstração de funcionalidades: Serviços e termos de engajamento, definição de fatores de sucesso, introdução a ferramenta e definição de pontos focais de contato

3.1.721. Revisão de Serviços: Relatórios de resultados da implementação, verificação de ferramenta implementada.

3.1.722. A CONTRATADA em conjunto com a CONTRATANTE realizará todas as atividades necessárias durante o processo de integração.

3.1.723. A CONTRATANTE deve: a) ter uma conta para visualização do portal da ferramenta de Serviço de Monitoramento proativo e resposta gerenciada válida e ativa, b) implantar e configurar o Software de Serviço aplicável em Endpoints Gerenciados, c) manter conformidade com todos os requisitos identificados nas Verificações de Saúde, e d) atender aos requisitos mínimos do sistema para instalar o Software de Serviço, e) configurar todos os Sistemas de Terceiros necessários para permitir a transmissão de toda a telemetria de segurança aplicável em um formato compatível com o Serviço; e f) executar apenas versões suportadas do Software de Serviço e/ou ferramentas de segurança de terceiros.

3.1.724. A CONTRATANTE reconhece e concorda que o Software de Serviço deve ser implantado em pelo menos oitenta por cento (80%) do volume licenciado, pois isso é necessário para fornecer à Equipe de Serviços de Segurança uma visibilidade suficiente no ambiente da CONTRATANTE para a entrega do Serviço. A CONTRATADA não será responsável ou responsabilizada por quaisquer problemas causados pela falha da CONTRATANTE em configurar ou habilitar as configurações de segurança disponibilizadas pela equipe da CONTRATADA ou por quaisquer problemas causados pela falha da CONTRATANTE em cumprir quaisquer requisitos aplicáveis.

3.1.725. A CONTRATANTE deve fazer esforços razoáveis para remediar prontamente quaisquer comprometimentos relatados pelo Serviço de Monitoramento proativo e resposta gerenciada. A CONTRATADA não será responsável ou responsabilizada por quaisquer problemas causados pela falha da CONTRATANTE em tomar medidas de remediação de forma oportuna.

3.1.726. A Equipe de Serviços de Segurança não tem obrigação de notificar a CONTRATANTE ou gerar novos Casos a partir de Detecções para as quais a CONTRATADA já forneceu etapas de remediação recomendadas.

3.1.727. Suporte Técnico

3.1.728. Durante o período de garantia contratual deverão estar cobertos, sem ônus adicionais, a prestação pela contratada, dos serviços de suporte e assistência técnica on-site, nas instalações da contratante, atendendo os seguintes requisitos:

3.1.729. A assistência técnica, suporte e gerenciamento a serem fornecidos junto com a implementação da solução deverá ser prestada, durante 12 meses referentes ao licenciamento e 24 meses de hardware referente aos equipamentos.

3.1.730. Atendimento inicial no prazo máximo de 04 (quatro) horas corridas, contadas a partir do instante do chamado feito pela contratante à contratada, por telefone, e-mail ou portal de atendimento on-line;

3.1.731. Conclusão do atendimento, com a resolução do problema que originou o chamado, no máximo de 16 (dezesseis) horas úteis, contadas a partir do instante do chamado feito pela contratante à contratada;

3.1.732. O suporte técnico deverá ser prestado pela contratada por telefone, e-mail, acesso remoto ou com a presença de seus técnicos on-site nas instalações da contratante, conforme a necessidade de cada demanda registrada.

3.1.733. Ainda poderão ser executadas as seguintes tarefas em relação a prestação de suporte:

3.1.734. Orientação de procedimentos operacionais para o funcionamento e uso adequado da solução fornecida pela contratada como: Resolução de dúvidas sobre o produto, Discussão de melhorias na configuração, Resolução de pequenos problemas e ajustes na solução.

3.1.735. A Contratada deverá prover todo o suporte e gestão da solução ofertada.

3.1.736. É responsabilidade da Contratada monitorar a solução 24x7x365 (vinte e quatro horas, sete dias por semana, 365 dias por ano) para garantia da disponibilidade da mesma.

3.1.737. A solução proposta deverá prever medidas para garantir a proteção dos dados, antecipando ameaças à privacidade, segurança e integridade, prevenindo acesso não autorizado às informações.

3.1.738. Em casos de paralisações dos serviços deve a Contratada iniciar a correção do problema em até 4 (quatro) horas corridas.

3.1.739. Tabela de SLA (Monitoramento e Alerta de Incidentes) - As seguintes definições se aplicam para o SLA:

3.1.740. "Alta Severidade" um caso criado a partir de Detecções geradas automaticamente por políticas ou análises aplicadas à telemetria de Endpoints Gerenciados que é determinado como de alta ou crítica severidade após revisão da equipe dos serviços de Monitoramento proativo e resposta gerenciada;

3.1.741. "Tempo de Resposta" é o tempo decorrido entre a identificação de um Caso de Alta Severidade e o momento em que a Equipe dos serviços de Monitoramento proativo e resposta gerenciada inicia: (i) contato para notificar a CONTRATANTE sobre tal Caso de Alta Severidade, por e-mail ou telefone;

3.1.742. O Tempo de Resposta deverá ser de até sessenta (60) minutos para oitenta e oito porcento (88%) dos Casos de Alta Severidade medidos mensalmente. Caso a CONTRATADA não cumprir o Tempo de Resposta acima mais de três vezes em qualquer período de doze (12) meses consecutivos, será considerada uma falha no SLA.

3.1.743. Caso a CONTRATADA não cumpra o SLA conforme descrito acima, a CONTRATANTE terá direito a um crédito no valor de cinco por cento (5%) das taxas pagas pelo Serviço durante o ciclo de faturamento anterior, ou cinco mil dólares ($5,000), o que for menor. O Crédito de Serviço deverá ser aplicado à taxa de assinatura para o próximo período de assinatura do Serviço. Caso a CONTRATANTE possua direito ao Crédito de Serviço e permitir que a assinatura expire por qualquer período após o término do período de assinatura, então o Crédito de Serviço será perdido.

3.1.744. A CONTRATANTE deve poder reivindicar um Crédito de Serviço até três (3) vezes em qualquer ano calendário.

3.1.745. Para qualquer um dos níveis de Serviço mencionados acima, a CONTRATANTE reconhece e concorda que, além das ações exigidas da CONTRATANTE, esta, deve tomar as seguintes ações para facilitar e permitir a entrega do Serviço, a CONTRATADA não terá responsabilidade por qualquer entrega de Serviço degradada, incompleta ou falha que possa resultar da falha da CONTRATANTE em realizar as ações necessárias. A CONTRATADA reserva-se o direito de suspender a entrega do Serviço até que a CONTRATANTE execute as ações necessárias. A falha em completar as ações necessárias após aviso por escrito (incluindo aviso por e-mail da Equipe de Serviços de Segurança para os contatos designados da CONTRATANTE) constituirá uma violação material pelo CONTRATANTE do Acordo.

3.1.746. A CONTRATANTE deve garantir que todos os Endpoints Gerenciados tenham configurações de hora e data precisas. A CONTRATADA não será responsável por erros, problemas e riscos residuais experimentados ou incorridos pela CONTRATANTE para Detecções geradas por Endpoints Gerenciados com configurações de hora e data imprecisas.

3.1.747. Tempo máximo para criação de caso após a detecção do Serviço de monitoramento proativo e resposta gerenciada deverá ser no máximo de 4 minutos.

3.1.748. Tempo máximo para resposta inicial após a detecção Serviço de monitoramento proativo e resposta gerenciada deverá ser no máximo de 40 minutos.

3.1.749. Os incidentes criados devem seguir a seguinte tabela de classificação de severidade:

Severidade Definição Critica Uma confirmação de comprometimento ou acesso não autorizado ao(s) sistema(s) que representa uma ameaça iminente aos ativos, incluindo atacantes interativos, criptografia ou destruição de dados e exfiltração.

Alta Detecções que indicam um ataque direcionado com o potencial de causar um comprometimento confirmado ou acesso não autorizado ao(s) sistema(s) que representará uma ameaça iminente aos ativos.

Media Detecções que podem não ser consideradas maliciosas por si só e não são conhecidas por serem direcionadas.

Baixa Detecções que não indicaram problemas, atividade maliciosa, ou comprometimento confirmado ou acesso não autorizado ao(s) sistema(s).

Informativa Uma severidade especial para as Verificações iniciais de comprometimento.

3.1.750. A Contratada será responsável por operar as tarefas das soluções de acordo com as solicitações realizadas pela equipe de TI da Contratante, devendo adicionar, alterar ou remover tarefas e rotinas das soluções, de acordo com as informações fornecidas pela equipe de TI da Contratante.

3.1.751. A Contratada será responsável em verificar a execução das rotinas e tarefas das soluções.

3.1.752. Em casos de falha, a Contratada deverá notificar prontamente a equipe de TI da Contratante, verificar a causa raiz da falha, e sendo possível a correção, corrigir e executar novamente a tarefa.

3.1.753. Em casos de impossibilidade técnica da resolução do erro, a Contratada deve abrir chamado juntamente com a equipe de TI da Contratante para que o erro possa ser solucionado.

3.1.754. A assistência técnica e suporte a serem fornecidos junto com a implementação da solução deverá ser prestada, durante 12 meses referente ao licenciamento e 24 meses referentes ao Hardware;

3.1.755. Durante o período de garantia contratual deverão estar cobertos, sem ônus adicionais, a prestação pela contratada, dos serviços de suporte e assistência técnica on-site, nas instalações da contratante, atendendo os seguintes requisitos:

3.1.756. Atendimento inicial no prazo máximo de 04 (quatro) horas corridas, contadas a partir do instante do chamado feito pela contratante à contratada, por telefone, e-mail ou portal de atendimento on-line;

3.1.757. Conclusão do atendimento, com a resolução do problema que originou o chamado, no máximo de 16 (dezesseis) horas úteis, contadas a partir do instante do chamado feito pela contratante à contratada;

3.1.758. O suporte técnico deverá ser prestado pela contratada por telefone, e-mail, acesso remoto ou com a presença de seus técnicos on-site nas instalações da contratante, conforme a necessidade de cada demanda registrada.

3.1.759. Ainda poderão ser executadas as seguintes tarefas em relação a prestação de suporte:

3.1.760. Orientação de procedimentos operacionais para o funcionamento e uso adequado da solução fornecida pela contratada;

3.1.761. Resolução de dúvidas sobre o produto;

3.1.762. Discussão de melhorias na configuração;

3.1.763. Resolução de pequenos problemas e ajustes na solução.

3.1.764. A Contratada deverá prover todo o suporte e gestão da solução ofertada.

3.1.765. A solução proposta deverá prever medidas para garantir a proteção dos dados, antecipando ameaças à privacidade, segurança e integridade, prevenindo acesso não autorizado às informações.

3.1.766. Em casos de paralisações dos serviços deve a Contratada iniciar a correção do problema em até 4 (quatro) horas corridas.

3.1.767. A Contratada deverá fornecer suporte técnico 24x7, em língua portuguesa, para sanar dúvidas quanto da solução, sua configuração ou quaisquer outros assuntos relacionados as soluções.

3.1.768. O suporte técnico deverá ser realizado pelos seguintes canais de atendimento:

3.1.769. Webmail corporativo;

3.1.770. Sistema online de chamados para abertura de ticket.

3.1.771. Atendimento por número telefônico gratuito (0800), para atendimento dos usuários, visando garantir acesso facilitado e imediato a equipe de suporte técnico;

3.1.772. Comprovação em sede de proposta, por meio de indicação dos canais de comunicação de que possui funcionamento e atendimento 24x7x365, com funcionamento de capacidade de operação ininterrupta.

3.1.773. Em casos de desastre, restaurações de bancos ou que seja necessária a restauração de um ou mais servidores, a Contratada deve analisar, e se necessário, disponibilizar time técnico presencial nas dependências da Contratante para a realização ou acompanhamento das tarefas.

3.1.774. A Contratada deverá enviar mensalmente relatório estatístico das rotinas das soluções.

3.1.775. É responsabilidade da Contratada o acompanhamento do uso e o planejamento de capacidade do mesmo, informando mensalmente a Contratante as estatísticas de uso e situação corrente, a previsão de crescimento com base nos dados históricos e possíveis inadequações do ambiente ao crescimento esperado.

3.1.776. Deverá revisar e atuar de forma proativa na console de gestão diariamente com o intuito de evitar possíveis ameaças;

3.1.777. A CONTRATADA deverá apresentar, no início do contrato, toda a documentação e os procedimentos para acionamento do suporte técnico.

3.1.778. O serviço deve incluir monitoramento proativo da plataforma pela CONTRATADA para identificar e corrigir possíveis falhas antes que impactem os usuários.

3.1.779. Em até 5 (cinco) dias após a assinatura de contrato, a CONTRATADA iniciará a prestação do serviço, a partir da data de emissão da ordem de serviço pela SECTI.

3.1.780. Todos os serviços relativos aos acessos a Plataforma de Gestão do Equipamento, serão de responsabilidade da Empresa CONTRATADA, sem ônus para a SECTI.

3.1.781. A configuração para a gestão e disponibilização dos acessos aos usuários, será realizada pela CONTRATADA em conjunto com os Técnicos do Departamento de Projetos, Redes, Segurança e Sistemas da Secretaria Municipal de Ciência e Tecnologia.

3.1.782. Os serviços serão recebidos provisoriamente após a ativação da plataforma e a validação, pela equipe técnica da Secretaria Municipal de Ciência e Tecnologia e Inovação, de que todas as funcionalidades contratadas estão operacionais.

4. REQUISITOS DE CONTRATAÇÃO:

4.1. A contratação refere-se à aquisição remunerada de bens comuns, para fornecimento de uma só vez, cujos padrões de desempenho e qualidade foram objetivamente definidos por meio de especificações usuais de mercado, devendo ser contratado mediante licitação, na modalidade de pregão, na forma eletrônica, pelo critério de julgamento menor preço por item.

4.2. A licitante deverá possuir e comprovar juntamente com os documentos de habilitação:

4.3. Possuir em seu quadro de funcionários pelo menos 02 (dois) profissionais nível igual ou similar a Engenheiro (Enginner) para mitigação de riscos, bem como o devido manuseio da solução e suporte a equipe de TI.

4.4. Também comprovar que possui no mínimo 02 (dois), profissional nível arquiteto certificado nas soluções de Endpoint e Firewall propostas, que integre a equipe de trabalho, para assegurar o pleno funcionamento e a eficiência operacional do projeto, contribuindo para a continuidade dos serviços de tecnologia da informação oferecidos, sendo admitida a apresentação de mais de um profissional.

4.5. Deve apresentar a comprovação (declaração ou certificação) emitida pelo fabricante do software ofertado, declarando que a empresa licitante está autorizada a comercializar e gerenciar as subscrições ofertadas para este Certame.

4.6. Para fins de comprovação de aderência do equipamento ofertado, poderá ser solicitado pela equipe técnica, apresentação de documento (ponto a ponto) que indique a devida descrição de cada item que compõe o descritivo técnico dos produtos ofertados, indicando no manual/catálogo do fabricante a aderência do produto aos requisitos das especificações técnicas.

4.7. Com relação à QUALIFICAÇÃO TÉCNICA, deverá o licitante apresentar a expertise na solução além de comprovação de fornecimento deste serviço a outros órgãos/ instituições compatíveis com o fornecimento solicitado.

4.8. O fabricante da solução deverá fornecer, obrigatoriamente, uma carta oficial de parceria emitida diretamente pelo fabricante, atestando a validade e a categoria da parceria, não sendo aceitos prints de informações provenientes de sites ou outras fontes não oficiais. A carta de parceria deverá ser datada, assinada por representante autorizado do fabricante.

4.9. Também comprovar que possui no mínimo 01 (um) especialista na solução de firewall e endpoint ofertadas, por meio de certificações da fabricante, que integre a equipe de trabalho, para assegurar o pleno funcionamento e a eficiência operacional do projeto, contribuindo para a continuidade dos serviços de tecnologia da informação oferecidos.

4.10. Deve apresentar a comprovação (declaração) emitida pelo fabricante do software ofertado, declarando que a empresa licitante está autorizada a comercializar e gerenciar as subscrições ofertadas para este Certame.

4.11. Para fins de comprovação de aderência do equipamento ofertado, caso haja necessidade poderá ser solicitada ao licitante a apresentação de documento (ponto a ponto) que indique a devida descrição de cada item que compõe o termo de referência, juntamente com a proposta, indicando no manual/catálogo do fabricante a aderência do produto aos requisitos das especificações técnicas.

4.12. Prova de capacidade técnica, mediante apresentação de certidão(ões) ou atestado(s) fornecido(s) por pessoas jurídicas de direito público ou privado, demonstrando fornecimento de produtos pertinentes e compatíveis com o objeto deste termo;

5. MODELO DE EXECUÇÃO DO OBJETO:

5.1. FORMA DE FORNECIMENTO:

5.1.1 A entrega do objeto será no prazo máximo de até 30 (trinta) dias corridos após o recebimento da ordem de fornecimento.

5.1.2 Endereço de entrega: O objeto deverá ser entregue no seguinte endereço: Rua Comendador Sá, 96, Centro, Piraí, RJ, CEP 27.175-000, de segunda a sexta-feira, exceto feriados, sem ônus de frete e seguro para o município;

Horário para entrega: das 08h00min às 12h00min e das 13h00min às 17h00min;

Telefone para contato: (24) 2431-9952/ 9962.

5.1.3 O prazo de garantia dos produtos, contra defeitos de fabricação, será de, no mínimo, 12 (doze) meses, a partir da data de entrega;

5.1.4 Após 30 (trinta) dias de atraso na entrega do objeto a partir do prazo estabelecido, sem que haja justificativa aceita pela fiscalização da contratante, o contrato poderá ser rescindido e o empenho anulado, ficando o fornecedor sujeito às sanções previstas.

5.1.5 O dispositivo de firewall deverá ser compatível com os estudos técnicos de viabilidade e com as análises de desempenho previamente realizadas por equipe especializada, de modo a assegurar o atendimento adequado à sobrecarga máxima de utilização prevista.

5.1.6 A solução deverá ser dimensionada com base em cenários de uso extremo, considerando picos de tráfego, simultaneidade de acessos e condições críticas de operação, garantindo desempenho, estabilidade e continuidade dos serviços.

5.1.7 O acesso à plataforma de gestão dos dispositivos Ethernet Remotos será via navegador web e deverá ser integrada ao Sistema de Firewall Sophos existente na Prefeitura Municipal de Piraí. Deverá ser repassada todas as informações para acesso do produto.

5.1.8 O prazo de garantia dos serviços de software será de, no mínimo, 12 (doze) meses, correspondente à vigência do contrato.

6.CONDIÇÕES DE RECEBIMENTO DO OBJETO:

6.1.1 Os bens e serviços objeto deste Termo de Referência serão recebidos e aceitos, de acordo com o art. 140 da lei n. 14.133/2021, provisoriamente, após sumária inspeção realizada pela Fiscalização da Secretaria Municipal Ciência e Tecnologia, para posterior verificação da qualidade e conformidade do objeto às especificações técnicas exigidas neste termo, podendo ser rejeitados caso não estejam conforme as especificações estabelecidas.

6.1.2 A contratada deverá dar total garantia quanto à qualidade dos bens fornecidos e serviços executados, ficando obrigada a reparar, corrigir ou substituir às suas expensas, no total ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções comprovadamente fora das especificações técnicas discriminadas no presente termo.

6.1.3 Os bens e serviços serão recebidos definitivamente no prazo de 15 (quinze) dias, após do termino do prazo estabelecido no contrato, por servidor ou comissão designada pela autoridade competente, mediante termo detalhado que comprove o atendimento das condições e especificações discriminadas no Termo de Referência.

7.MODELO DE GESTÃO DO CONTRATO:

7.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e nos termos da Lei n. 14.133/2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial;

7.2. A execução do contrato será acompanhada e fiscalizada por servidor(es) especialmente designado(s) em portaria da **Secretaria Municipal de Ciência e Tecnologia;**

7.3. O fiscal do contrato anotará em registro próprio todas as ocorrências relacionadas à execução do contrato, determinando o que for necessária para regularização da falta ou defeitos observados.

7.4. As comunicações entre Contratante e Contratada devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim;

7.5. O fiscal do contrato informará, em tempo hábil, ao superior do seu departamento ou setor, a situação que demandar decisão ou providência que ultrapasse a sua competência;

7.6. O fiscal do contrato será auxiliado pelos órgãos de assessoramento jurídico e de controle interno da Administração, que deverá dirimir dúvidas e subsidiá-lo com informações relevantes para prevenir riscos na execução contratual;

7.7. A contratante poderá convocar representante da Contratada para adoção de providências que deixem de ser cumpridas de imediato.

8. CONDIÇÕES DE PAGAMENTO:

8.1. O pagamento será efetuado no 30º (trigésimo) dia, a contar da data final do período de adimplemento do objeto, assim considerada a entrega do objeto, acompanhada do respectivo documento de cobrança (nota fiscal/fatura) devidamente atestada pela Fiscalização;

8.2. Os pagamentos serão efetuados, obrigatoriamente, por meio de crédito em conta corrente, cujo número e agência deverão ser informados pelo adjudicatário até a assinatura do contrato;

8.3. Os prestadores de Serviço e fornecedores de bens, deverão emitir as notas fiscais em observância ás regras de retenção, dispostas na Instrução Normativa RFB n° 1234, de 11 de janeiro de 2012, sob pena de não aceitação.

8.4. A retenção do imposto de renda deverá ser destacada no corpo do documento fiscal observando os percentuais estabelecidos no anexo I da Instrução Normativa RFB nº 1.234/2012.

8.5. As pessoas jurídicas amparadas por isenção, não incidência ou alíquota zero devem informar essa condição no documento fiscal, inclusive o enquadramento legal, sob pena de, se não o fizerem, sujeitarem-se à retenção do imposto de renda sobre o valor total do documento correspondente à natureza do bem ou serviço

8.6. Havendo erro na apresentação da nota fiscal ou instrumento de cobrança equivalente, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus ao contratante;

8.7. Em caso de atraso injustificado no pagamento, o valor será compensado financeiramente em 0,5% (cinco décimos por cento) de juros de mora por mês “pro rata tempore”, contados a partir do dia seguinte ao seu vencimento até a data do efetivo pagamento;

9. FORMA E CRITÉRIO DE SELEÇÃO DO FORNECEDOR:

9.1. O fornecedor será selecionado por meio da realização de licitação, na modalidade de pregão, sob a forma eletrônica, com adoção do critério de julgamento pelo menor preço global, observados os preços **unitários** máximos admitidos e a compatibilidade da proposta com a especificação técnica do objeto.

Prefeitura Municipal de Piraí – APROVADO – Assessoria Jurídica

Prefeitura Municipal de Piraí – Secretaria Municipal Administração – Estado do Rio

10. ESTIMATIVA DO VALOR DA CONTRATAÇÃO:

10.1. O custo estimado global da presente contratação é de **R$ 223.000,00** (Duzentos e vinte e três mil reais).

10.2. Data base dos orçamentos: Julho/2026.

11. ADEQUAÇÃO ORÇAMENTÁRIA:

11.1. A despesa com a execução do objeto deste termo de referência correrá pela dotação orçamentária:

11101957200142213339040001500000
11101957200142213449052001500000

12. IMPACTO E SUSTENTABILIDADE AMBIENTAL

12.1. A contratada deverá cumprir as orientações descritas no **art. 5°** e **art. 6°** da Instrução Normativa n° 1, de 19/01/2010, do Ministério Do Planejamento, Desenvolvimento e Gestão (MPDG), no que couber, além dos critérios eventualmente inseridos na especificação do objeto.

13. SANÇÕES:

13.1. No caso de descumprimento total ou parcial das condições estabelecidas no presente Termo de Referência, a contratada estará sujeita à aplicação das penalidades previstas nos artigos 155 a 163 da Lei Federal n. 14.133/2021.

Prefeitura Municipal de Piraí – APROVADO – Assessoria Jurídica

Prefeitura Municipal de Piraí – Secretaria Municipal Administração – Estado do Rio

Elaborado por:

Larissa Lima Ofrede Setor de Compras Matrícula: 13018

Responsável (is) por especificações técnicas e quantitativas:

Tercio Passos da Fonseca Mat.: 9133 Chefe Div. de Des. Programas e Projetos	**Patryck Soares de Moura Barbosa** Mat.: 9141 Analista de Suporte

Aprovo o presente Termo de Referência, que constitui peça integrante e inseparável do procedimento licitatório objetivando Aquisição de solução integrada (Harwdware/Software) de Firewall de Próxima Geração Tipo 1, conforme condições e especificações contidas neste Termo de Referência.

Secretário de Administração

ANEXO II
MODELO DE PROPOSTA

AO
MUNICÍPIO DE PIRAÍ
Praça Getúlio Vargas, S/Nº
Centro - Piraí - R.J.

Ref.: Pregão Eletrônico nº _____/2026

A empresa _____, com endereço na _____, nº ____ - Bairro _____ - Cidade _____, CNPJ nº _____, telefone _____, pela presente, propõe a prestar os serviços descritos no quadro abaixo, obedecendo as normas do edital licitatório em referência, assim como seus anexos, conforme condições seguintes:

ITEM	*QUANT*	*UNID*	*DESCRIÇÃO*	*PREÇO UNIT(R$)*	*PREÇO TOTAL(R$)*
VALOR GLOBAL (R$)					

Preço Global: __.____,__ (__preço por extenso__)

Forma de execução conforme disposto no Termo de Referência, Anexo I deste Edital

Condições de pagamento: Conforme disposto no Termo de Referência, Anexo I deste Edital

Validade da Proposta: 60 (sessenta) dias, a contar da data de realização desta licitação.

A proposta de preços deverá ser feita em moeda corrente nacional, englobando todas as despesas necessárias para a perfeita execução do objeto, tais como: mão de obra, materiais, equipamentos, carga e descarga, frete, estadia e alimentação dos funcionários, se for o caso, impostos, taxas ou quaisquer outros ônus federais, estaduais ou municipais, bem como o lucro.

Declaramos ainda que temos total conhecimento e concordância com os termos deste Pregão.
Dados Bancários: Agência ____, Conta Corrente _____, Banco _____.

_____, ____ de _____de _____

_____
Nome e assinatura do representante legal

OBS.: **A SER APRESENTADA APÓS A DISPUTA E READEQUADA AO ÚLTIMO LANCE.**

Prefeitura Municipal de Piraí – Assessoria Jurídica – APROVADO
Prefeitura Municipal de Piraí – Secretaria Municipal Administração – Estado do Rio

ANEXO III
MINUTA DE CONTRATO

CONTRATO Nº _____/2026

Termo de Contrato nº _____/2026 para a Prestação de serviço de _____, entre o Município de Piraí e a Empresa_____.

O Município de Piraí, inscrito no CNPJ sob o nº. 29.141.322/0001-32, com sede à Praça Getúlio Vargas, s/nº - Centro – Piraí/RJ doravante denominado CONTRATANTE, neste ato representada pelo Prefeito Municipal Sr._____, portador da Carteira de Identidade Nº._____ expedida pelo_____, CPF n°._____, de um lado, e, do outro, a empresa _____, inscrita no CNPJ sob o n° _____, com sede na _____, nº ____, bairro _____, _____, ____, CEP: _____, doravante denominada CONTRATADA, representada neste ato por _____, _____, _____, _____, portador da carteira de identidade n° _____, expedida pelo _____, e do CPF n° _____, residente e domiciliado na _____, assinam o presente **CONTRATO**, de conformidade com o que consta do Processo Administrativo nº _____/_____/2026, que se regerá, no que couber, pelas normas da Lei Federal nº 14.133/2021 com as alterações introduzidas posteriormente e pelas cláusulas e condições que se seguem:

CLÁUSULA PRIMEIRA – DO OBJETO:

O presente contrato tem por objeto a prestação de serviço de _____, conforme especificações discriminadas no Termo de Referência – Anexo I do edital de Pregão Eletrônico nº _____/2026.

CLÁUSULA SEGUNDA – DO VALOR:

O preço global deste contrato é de **R$** _____ (..), conforme proposta da **CONTRATADA** discriminada no quadro abaixo:

ITEM	*QUANT*	*UNID*	*DESCRIÇÃO*	*PREÇO UNIT(R$)*	*PREÇO TOTAL(R$)*
VALOR GLOBAL (R$)					

PARÁGRAFO ÚNICO: O valor ajustado incluir todos os custos de: mão de obra, materiais e equipamentos, carga e descarga, frete, impostos, taxas ou quaisquer outros ônus federais, estaduais

Prefeitura Municipal de Piraí APROVADO Assessoria Jurídica

Prefeitura Municipal de Piraí Secretaria Municipal Administração Estado do Rio

ou municipais, incluídos, bem como o lucro enfim, tudo o que for necessário para a perfeita execução deste contrato.

CLÁUSULA TERCEIRA – DOS RECURSOS ORÇAMENTÁRIOS:

As despesas decorrentes do presente Contrato serão atendidas através da dotação orçamentária nº _____.

CLÁUSULA QUARTA – DO REAJUSTE DE PREÇOS:

PARÁGRAFO PRIMEIRO: O(s) preço(s) previsto(s) na cláusula segunda será(ão) fixo(s) e irreajustável(is), inexistindo a possibilidade de adoção pelas partes de qualquer espécie de reajuste financeiro, em que a periodicidade de aplicação seja inferior a um período de 12 (doze) meses, em conformidade com o disposto no parágrafo 1°, do art. 2º da Lei Federal nº 10.192/01.

PARÁGRAFO SEGUNDO: Após o interregno de um ano, os preços iniciais poderão ser reajustados, mediante a aplicação, da variação do IPCA no período, de acordo com a data base vinculada à data do orçamento estimado, em _____/2026.

PARÁGRAFO TERCEIRO: Será assegurado a **CONTRATADA** a revisão de preços para reestabelecimento do equilíbrio econômico-financeiro do contrato, mediante prévia comprovação e justificativas submetidas à apreciação à Administração, em caso de força maior, caso fortuito, fato do príncipe ou em decorrência de fatos imprevisíveis ou previsíveis de consequências incalculáveis, que inviabilizem a execução do contrato tal como pactuado, respeitada, em qualquer caso, a repartição objetiva de risco estabelecida no contrato, conforme previsto na alínea d do inciso II do artigo 124 da Lei Federal 14.133/21.

CLÁUSULA QUINTA – DA EXECUÇÃO DO OBJETO:

I. Os serviços objeto deste contrato deverão ser executados atendendo todas as especificações contidas no Termo de Referência, anexo I do edital do pregão eletrônico nº _____, que integra o presente contrato, independente de transcrição.

II. O contratado fica obrigado a manter, durante toda a execução do contrato, em compatibilidade com as obrigações por ele assumidas, todas as condições exigidas para a habilitação.

CLÁUSULA SEXTA – DO RECEBIMENTO DO OBJETO:

I. Os serviços objeto deste contrato serão recebidos e aceitos, de acordo com o art. 140 da lei nº 14.133/2021, após sumária inspeção realizada pela Fiscalização da Secretaria solicitante, para posterior verificação da qualidade e conformidade do objeto às especificações técnicas discriminadas no termo de referência, anexo I deste edital, podendo ser rejeitados caso não estejam conforme as especificações estabelecidas.

II. A **CONTRATADA** deverá dar total garantia quanto à qualidade do objeto executado, ficando obrigada a substituir às suas expensas, no total ou em parte, os serviços em que se verificarem vícios, defeitos ou incorreções comprovadamente fora das especificações técnicas discriminadas.

III. O objeto será recebido definitivamente no prazo de 15 (quinze) dias, contados do recebimento provisório, por servidor ou comissão designada para fiscalização, mediante termo detalhado que comprove o atendimento das condições e especificações discriminadas no Termo de Referência.

CLÁUSULA SÉTIMA – DA GESTÃO E FISCALIZAÇÃO DO CONTRATO:

I. A execução do presente contrato será fiscalizada por servidor especialmente designado em Portaria da Secretaria solicitante, de acordo com o disposto no art. 117, da Lei Federal nº 14.133/2021.

II. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

III. O fiscal do contrato anotará em registro próprio todas as ocorrências relacionadas à execução do contrato, determinando o que for necessária para regularização da falta ou defeitos observados.

IV. As comunicações entre **CONTRATANTE** e **CONTRATADA** devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

V. O fiscal do contrato informará, em tempo hábil, ao superior do seu departamento ou setor, a situação que demandar decisão ou providência que ultrapasse a sua competência.

VI. O fiscal do contrato será auxiliado pelos órgãos de assessoramento jurídico e de controle interno da Administração, que deverá dirimir as dúvidas e subsidiá-lo com informações relevantes para prevenir riscos na execução contratual.

VII. A **CONTRATANTE** poderá convocar representante da **CONTRATADA** para adoção de providência que deixem de ser cumpridas de imediato.

VIII. A **CONTRATADA** será responsável pelos danos causados diretamente à Administração ou a terceiros em razão da execução do contrato, e não excluirá nem reduzirá essa responsabilidade a fiscalização ou o acompanhamento pela **CONTRATANTE**;

IX. A **CONTRATADA** fica obrigada a aceitar nas mesmas condições contratuais, os acréscimos ou diminuição quantitativa de seu objeto, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

X. As alterações contratuais deverão ser formalizadas por termo aditivo, exceto registros que não caracterizam alteração no contrato, que poderão ser formalizados por simples apostila, de acordo com as situações previstas no art. 136 da Lei Federal nº14.133/2021.

CLÁUSULA OITAVA – DAS CONDIÇÕES DE PAGAMENTO:

A **CONTRATANTE** efetuará o pagamento no 30º (trigésimo) dia, a contar da data final do período de adimplemento do objeto, assim considerada a execução do objeto, acompanhada do respectivo documento de cobrança (nota fiscal/fatura) devidamente atestada pela Fiscalização.

PARÁGRAFO PRIMEIRO: O pagamento será efetuado, obrigatoriamente, por meio de crédito em conta corrente, cujo número e agência deverão ser informados pela **CONTRATADA**.

PARAGRAFO SEGUNDO: A retenção do imposto de renda deverá ser destacada no corpo do documento fiscal observando os percentuais estabelecidos no anexo I da Instrução Normativa RFB nº 1.234/2012.

PARÁGRAFO TERCEIRO: As pessoas jurídicas amparadas por isenção, não incidência ou alíquota zero devem informar essa condição no documento fiscal, inclusive o enquadramento legal, sob pena de, se não o fizerem, sujeitarem-se à retenção do imposto de renda sobre o valor total do documento correspondente à natureza do bem ou serviço

PARÁGRAFO QUARTO: Havendo erro na apresentação da nota fiscal ou instrumento de cobrança equivalente, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que a **CONTRATADA** providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus a **CONTRATANTE**.

PARÁGRAFO QUINTO: Em caso de atraso injustificado no pagamento, o valor será compensado financeiramente em 0,5% (cinco décimos por centos) de juros de mora por mês "pro rata tempore", contados a partir do dia seguinte ao seu vencimento até a data do efetivo pagamento.

CLÁUSULA NONA – DA VIGÊNCIA CONTRATUAL:

O prazo de prestação dos serviços objeto deste contrato será de 12 (doze) meses, a partir da ordem de serviço, podendo ter sua duração prorrogada a critério da Administração, tendo em vista tratar-se de serviço de natureza continuada de necessidade pública permanente a ser satisfeita, desde que os preços e condições sejam vantajosos para a Administração, nos termos do disposto no Art. 107, da Lei nº. 14.133/21.

CLÁUSULA DECIMA – DAS ALTERAÇÕES CONTRATUAIS:

PARÁGRAFO PRIMEIRO: O contrato poderá ser alterado, com as devidas justificativas, nos casos previstos no Art. 124, da Lei nº 14.133/21.

PARÁGRAFO SEGUNDO: Havendo alteração do contrato que aumente ou diminua os encargos da **CONTRATADA**, a **CONTRATANTE** deverá estabelecer, no mesmo termo aditivo o equilíbrio econômico-financeiro inicial.

PARÁGRAFO TERCEIRO: Os preços contratados serão alterados, para mais ou para menos, conforme o caso, se houver, após a data da apresentação da proposta, criação, alteração ou extinção de quaisquer tributos ou encargos legais ou a superveniência de disposições legais, com comprovada repercussão sobre os preços contratados.

PARÁGRAFO QUARTO: As alterações contratuais deverão ser formalizadas por termo aditivo, exceto registros que não caracterizam alteração no contrato, que poderão ser formalizados por simples apostila, de acordo com as situações previstas no art. 136 da Lei Federal nº14.133/2021.

CLÁUSULA DÉCIMA PRIMEIRA – DAS SANÇÕES ADMINISTRATIVAS:

Pelo cometimento das infrações previstas nos incisos I, II, III, V, VII, VIII, X e XII do art. 155, da Lei Federal nº 14.133/2021, a **CONTRATADA** será responsabilizada administrativamente com a aplicação das seguintes sanções:

I. Advertência – Caso dê causa a inexecução parcial do contrato, quando não se justificar a imposição de penalidade mais grave.

II. Impedimento de licitar e contratar no âmbito da Administração Pública direta e indireta do Município de Piraí, pelo prazo de até 03 (três) anos, sem prejuízo da rescisão unilateral do contrato, quando praticar as seguintes infrações e não justificar a imposição de penalidades mais grave:

   a. Der causa a inexecução parcial do contrato que cause danos grave a Administração, ao fornecimento dos Serviços Públicos e ao interesse coletivo;

   b. Der causa a inexecução total do contrato;

   c. Ensejar o retardamento da execução/entrega do objeto do contrato sem motivo determinado.

III. Declaração de inidoneidade para licitar e contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos pelo prazo mínimo de 03 (três) anos e máximo de 05 (cinco) anos, quando praticar as seguintes infrações:

   a. Aquelas previstas para sanção de impedimento de licitar e contratar com o Município de Piraí, quando se justificar imposição de penalidade mais grave;

   b. Apresentar declaração ou documentação falsa durante a execução do contrato;

   c. Fraudar ou praticar ato fraudulento na execução do contrato;

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

   e. Praticar ato lesivo previsto no art. 5º da Lei Federal nº 12.846/2013.

IV. Multa compensatória e moratória que poderá ser aplicada sobre o valor do contrato, cumulativamente com as demais sanções por qualquer das infrações administrativas previstas nos incisos I, II, III, V, VII, VIII, X e XII do art. 155 da Lei Federal nº 14.133/2021.

V. A multa compensatória será aplicada no caso de execução parcial ou total do contrato, nos seguintes percentuais e condições:

a. No caso de inexecução parcial, será aplicado o percentual de 20% (vinte por cento) sobre o valor do contrato correspondente a parcela do objeto não executado;

b. No caso de inexecução total, será aplicado o percentual de 30% (trinta por cento) sobre o valor do contrato.

VI. A Multa de mora será de 0,5% (cinco décimos por cento) pro rata die sobre o valor do contrato, referente ao período de retardamento ou atraso na entrega/execução do objeto deste contrato, sem motivo justificado e aceito pela **CONTRATANTE**.

VII. A inexecução total do contrato estará configurada quando a **CONTRATADA**, deixar de cumprir o prazo referente a entrega/execução do objeto conforme as condições estabelecidas no presente contrato e termo de referência, anexo I do edital.

CLÁUSULA DÉCIMA SEGUNDA – DA EXTINÇÃO CONTRATUAL:

I. Constitui motivos para extinção do contrato, o qual deverá ser formalmente motivada nos autos do processo administrativo, assegurada o contraditório e a ampla defesa, as situações previstas no art. 137, incisos I, II, III, IV, V, VIII e IX da Lei Federal nº 14.133/2021.

II. A **CONTRATADA** terá direito a extinção do contrato, caso a Administração faça supressão modificando acima de 25% (vinte e cinco por cento) o valor inicial do contrato.

III. A extinção do contrato poderá ser determinada por ato unilateral da Administração, de forma consensual, ou por decisão arbitral, observando-se o disposto nos arts. 138 e 139 da Lei Federal nº14.133/2021.

CLÁUSULA DÉCIMA TERCEIRA – DAS DISPOSIÇÕES GERAIS:

I. Fazem parte integrante do presente contrato, o edital de Pregão Eletrônico nº _____/2026 e seus anexos, independente de transcrição.

II. Deverá a **CONTRATANTE** explicitamente emitir decisões de todas as solicitações e reclamações relacionadas ao contrato, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do contrato.

III. Concluída a instrução do requerimento, a Administração terá o prazo de 01 (um) mês para decidir, admitida a prorrogação motivada por igual período.

Prefeitura Municipal de Piraí – APROVADO – Assessoria Jurídica

Prefeitura Municipal de Piraí – Secretaria Municipal Administração – Estado do Rio

CLÁUSULA DÉCIMA QUARTA – DO FORO:

As partes contratantes, abrindo mão de qualquer privilegio, elegem o Foro da Comarca de Piraí, RJ, para dirimir as dúvidas oriundas deste contrato.

E, por estarem assim, justos e contratados, assinam o presente em 03 (três) vias de igual teor, na presença de duas testemunhas, para que produza seus jurídicos e legais efeitos.

Piraí, ____ de _____ de _____.

_____

MUNICÍPIO DE PIRAÍ

_____

CONTRATADA