PREGÃO ELETRÔNICO Nº 20240008– ETICE/DITEC

PROCESSO Nº 30032.000154/2024-71

UASG: 943001

Número Comprasnet: 91119/2024

A EMPRESA DE TECNOLOGIA DA INFORMAÇÃO DO CEARÁ – ETICE, por intermédio do pregoeiro e do membro da equipe de apoio designados por ato do Governador do Estado, que ora integra os autos, torna público que realizará licitação na modalidade PREGÃO, na forma eletrônica.

1. DO CRITÉRIO DE JULGAMENTO:

1.1. O critério de julgamento será o de Menor Preço por GRUPO, conforme tabela constante do Termo de Referência, devendo o licitante oferecer proposta para todos os itens que o compõe. A proposta final para o grupo não poderá conter item com valor superior ao estimado pela Administração, independentemente do valor total do grupo.

2. DA FORMA DE FORNECIMENTO:

2.1. A forma de fornecimento será parcelada.

3. DA BASE LEGAL

3.1. A licitação se encontra baseada na Lei Federal nº 14.133, de 1º de abril de 2021 e suas alterações; Lei Estadual nº 18.417, de 11 de julho de 2023; Lei Federal nº 14.682, de 20 de setembro de 2023, Lei Complementar nº 123, de 14 de dezembro de 2006; Lei Complementar Estadual nº 65, de 3 de janeiro de 2008, Lei Complementar Estadual nº 134, de 7 de abril de 2014, Decreto Estadual nº 35.067, de 21 de dezembro de 2022 e suas alterações, Decreto Estadual nº 35.283, de 19 de janeiro de 2023, Decreto Estadual nº 35.323 de 24 de fevereiro de 2023, Decreto Estadual nº 32.718, de 15 de junho de 2018; Decreto Estadual nº 27.624, de 22 de novembro 2004, Decreto Estadual nº 35.726, de 30 de outubro de 2023, Portaria PGE/GAB nº 36, de 8 de março de 2024, Regulamento de Licitações e Contratos da *Etice,* para as empresas públicas e as sociedades de economia mista, a Lei Federal nº 13.303, de 30 de junho de 2016, e demais legislações aplicáveis e, ainda, de acordo com as condições estabelecidas neste edital e seus anexos.

4. DO OBJETO

4.1. O objeto da licitação é o Registro de preços para futuras e eventuais aquisições de solução de proteção de redes, incluindo aquisições de hardware e software e respectivo serviço de implantação, posterior monitoramento e suporte técnico 24x7x365, contemplando utilização de equipamentos obrigatoriamente todos novos e de primeiro uso, de acordo com as especificações e quantitativos previstos neste termo.

5. DO ACESSO AO EDITAL, DO LOCAL DE REALIZAÇÃO E DO PREGOEIRO

5.1. Este edital está disponível gratuitamente nos sítios www.portalcompras.ce.gov.br e https://www.gov.br/compras/pt-br/acesso-a-informacao/consulta-detalhada.

5.2. O certame será realizado por meio do sistema do Comprasnet, no endereço eletrônico https://www.comprasnet.gov.br/seguro/loginPortal.asp, pelo pregoeiro Raimundo Lima de Souza.

5.3. Em atendimento à Portaria/PGE nº 038/2022, de 17 de março de 2022, a audiência que possa ser requerida por representante de licitante ou interessado em participar de licitação, com o fito de despachar sobre recurso ou impugnação de sua autoria junto à Central de Licitações, da Procuradoria-Geral do Estado, será realizada por meio presencial ou eletrônico e remoto, com o uso de solução tecnológica de videoconferência. Tal formalidade não se aplica no caso de simples instruções, tais como, provocações sobre datas, estágio de tramitação e demais orientações

meramente procedimentais, sem qualquer intervenção de mérito, que serão prestadas pela equipe de apoio da Central de Licitações, sob a supervisão de seu responsável.

5.3.1. A referida audiência realizar-se-á na presença de pelo menos 01 (um) Procurador do Estado, ou pela coordenação da Central de Licitações, de acordo com o caso, e deverá ser registrada em meio hábil à verificação do ato.

5.3.2. Observa-se que a solicitação de audiência deverá ser previamente encaminhada por e-mail, com indicação expressa do assunto e do processo licitatório a que relaciona. Quando realizada por meio eletrônico e remoto, a audiência deverá ficar registrada por meio de gravação e armazenamento de imagem e vídeo ou por redução a termo do ato.

5.3.3. A equipe de apoio atende pelo telefone de nº (85) 3459-6375 e pelo e-mail: licitacao@pge.ce.gov.br.

6. DAS DATAS E HORÁRIOS DO CERTAME

6.1. INÍCIO DO ACOLHIMENTO DAS PROPOSTAS: **21/11/2024**

6.2. DATA DE ABERTURA DAS PROPOSTAS……..: **03/12/2024, às 9h.**

6.3. INÍCIO DA SESSÃO DE DISPUTA DE PREÇOS: **03/12/2024, às 9h.**

6.4. REFERÊNCIA DE TEMPO: Para todas as referências de tempo utilizadas pelo sistema será observado o horário de Brasília/DF.

6.5. Na hipótese de não haver expediente ou ocorrendo qualquer fato superveniente que impeça a rea-lização do certame na data prevista, a sessão será remarcada, para no mínimo 48h (quarenta e oito horas) a contar da respectiva data, exceto quando remarcada automaticamente pelo próprio sistema eletrônico.

7. DO ENDEREÇO E HORÁRIO DA CENTRAL DE LICITAÇÕES

7.1. Central de Licitações/PGE, Av. Dr. José Martins Rodrigues, nº 150, Bairro Edson Queiroz, Fortaleza – Ceará, CEP. 60811- 520, CNPJ nº 06.622.070/0001-68.

7.2. Horário de expediente da Central de Licitações: das 8h às 12h e das 14h às 18h.

8. DA PARTICIPAÇÃO

8.1. Poderão participar deste certame os interessados que estiverem previamente credenciados no Sistema de Cadastramento Unificado de Fornecedores SICAF) disponível no Portal Nacional de Contratações Públicas (PNCP) e no Sistema de Compras do Governo Federal (www.gov.br/compras), por meio de Certificado Digital conferido pela Infraestrutura de Chaves Públicas Brasileira- ICP- Brasil.

8.1.1. A participação implica a aceitação integral dos termos deste edital.

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

8.3. O licitante responsabiliza-se exclusiva e formalmente pelas transações efetuadas em seu nome, assume como firmes e verdadeiras suas propostas e seus lances, inclusive os atos praticados diretamente ou por seu representante, excluída a responsabilidade do provedor do sistema ou da Central de Licitações responsável pelo processamento das licitações, por eventuais danos decorrentes de uso indevido das credenciais de acesso, ainda que por terceiros.

8.3.1. 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.

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

8.4. **Não poderão disputar esta licitação:**

8.5.1. Aquele que não atenda às condições deste edital e seus anexos;

8.5.2. Empresa em estado de insolvência civil, sob processo de falência, dissolução, fusão, cisão, incorporação e liquidação.

8.5.3. Pessoa física ou jurídica que se encontre, ao tempo da licitação, impossibilitada de participar da licitação em decorrência de sanção que lhe foi imposta, observado o § 1º do art. 14 da Lei nº 14.133/2021;

8.5.4. Agente público do órgão ou entidade licitante, 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, conforme §1º do art. 9º da Lei nº 14.133/2021. A vedação é estendida a terceiros que auxilie a condução da contratação na qualidade de integrante de equipe de apoio, profissional especializado ou funcionário ou representante de empresa que preste assessoria técnica.

8.5.5. Empresa estrangeira não autorizada a comercializar no país;

8.5.6. Empresa ou sociedade cooperativa cujo estatuto ou contrato social não inclua em seu objetivo social atividade compatível com o objeto do certame, e ainda, que não atendam o art. 16 da Lei nº 14.133/2021;

8.5.7. Organizações da Sociedade Civil de Interesse Público - OSCIP, atuando nessa condição;

8.5.8. Empresas controladoras, controladas ou coligadas, nos termos da Lei nº 6.404, de 15 de dezembro de 1976, concorrendo entre si;

8.5.9. Pessoa física ou jurídica que mantenha vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou 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;

8.5.10. Pessoa física ou jurídica que, nos 5 (cinco) anos anteriores à divulgação deste 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;

8.5.11. Pessoa física ou jurídica que integre o rol de pessoas sancionadas nas hipóteses do §5º do art.14 da Lei nº 14.133/2021, ou que seja declarada inidônea nos termos da referida Lei.

8.5.12. A participação de consórcio, qualquer que seja sua constituição.

9. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

9.1. Qualquer pessoa é parte legítima para impugnar este edital por irregularidade na aplicação da Lei nº 14.133/2021, ou para solicitar esclarecimento sobre seus termos, devendo encaminhar o pedido até 3 (três) dias úteis antes da data da abertura do certame, no endereço eletrônico citado no subitem 9.3 abaixo.

9.2. A resposta à impugnação ou ao pedido de esclarecimento será divulgada por meio do sistema utilizado na realização do certame, no prazo de até 3 (três) dias úteis contado da data de recebimento do pedido, limitado ao último dia útil anterior à data da sessão pública. As respostas divulgadas vincularão os participantes e a Administração.

9.2.1. As decisões do pregoeiro, se darão com embasamento nos pareceres e laudos emitidos pelas áreas técnicas e jurídicas do órgão e entidade promotora da licitação nos termos dos §§ 1º,

2º e 3º do art. 24 do Decreto nº 35.067/2022.

9.2.2. Na impossibilidade de resposta à impugnação no prazo citado no subitem 9.2, o pregoeiro poderá adiar a abertura da sessão pública, mediante aviso no sistema utilizado na realização do certame.

9.3. A impugnação e o pedido de esclarecimento deverão ser realizados exclusivamente por meio eletrônico, no endereço licitacao@pge.ce.gov.br, até as 23h59min, com a informação do nº do pregão, o órgão ou entidade promotor da licitação e pregoeiro responsável.

9.3.1. As impugnações apresentadas deverão ser subscritas por representante legal mediante comprovação, sob pena do seu não conhecimento.

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

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

9.5. Acolhida a impugnação, será definida e publicada nova data para a realização do certame, exceto quando a alteração não comprometer a formulação das propostas.

10. DA HABILITAÇÃO

10.1. A habilitação será verificada por meio do Sistema de Cadastramento Unificado de Fornecedores – SICAF, do Governo Federal ou do Certificado de Registro Cadastral (CRC) emitido pela Secretaria do Pla-nejamento e Gestão (SEPLAG), do Estado do Ceará, nos documentos de habilitação por eles abrangidos.

10.1.1. A verificação no Sistema de Cadastramento Unificado de Fornecedores(SICAF) ou a exigência dos documentos nele não contidos, somente será feita em relação ao licitante provisoriamente vencedor.

10.1.2. A verificação pelo pregoeiro, em sítios eletrônicos oficiais de órgãos e entidades emissores de certidões constitui meio legal de prova, para fins de habilitação.

10.1.3. Como condição prévia ao exame da documentação de habilitação do licitante detentor da proposta classificada em primeiro lugar, o pregoeiro verificará o eventual descumprimento das condições de participação previstas neste edital.

10.1.4. Constatada a existência de sanção e/ou eventual descumprimento das condições de participação, o pregoeiro reputará o licitante inabilitado.

10.2. **Habilitação jurídica**

10.2.1. A documentação relativa à habilitação jurídica consistirá em:

10.2.1.1. Pessoa física: cédula de identidade (RG) ou documento equivalente que, por força de lei, tenha validade para fins de identificação em todo o território nacional;

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

10.2.1.3. 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;

10.2.1.4. 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;

10.2.1.5. 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 n.º 77, de 18 de março de 2020.

10.2.1.6. Sociedade simples: inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;

10.2.1.7. 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;

10.2.1.8. Sociedade cooperativa: ata de fundação e estatuto social, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, além do registro de que trata o art. 107 da Lei nº 5.764/1971;

10.3. **HABILITAÇÂO TÉCNICA**

10.3.1. A documentação relativa à qualificação técnico-operacional consistirá em:

10.3.1.1. Comprovação de aptidão para o desempenho de atividade pertinente e compatível em características com o objeto da licitação, mediante apresentação de atestado(s) fornecido(s) por pessoa(s) jurídica(s) de direito público ou privado.

10.3.2. Para a participação de cooperativas, será exigida a seguinte documentação complementar:

10.3.2.1. A relação dos cooperados que atendem aos requisitos técnicos exigidos para a contratação e que executarão o contrato, com as respectivas atas de inscrição e a comprovação de que estão domiciliados na localidade da sede da cooperativa, respeitado o disposto nos arts. 4º, inciso XI, 21, inciso I e 42, §§2º a 6º da Lei nº 5.764/1971;

10.3.2.2. A declaração de regularidade de situação do contribuinte individual – DRSCI, para cada um dos cooperados indicados;

10.3.2.3. A comprovação do capital social proporcional ao número de cooperados necessários à execução do contrato;

10.3.2.4. O registro previsto no art. 107 da Lei nº 5.764/1971;

10.3.2.5. A comprovação de integração das respectivas quotas-partes por parte dos cooperados que executarão o contrato;

10.3.2.6. Os seguintes documentos para a comprovação da regularidade jurídica da cooperativa: a) ata de fundação; b) estatuto social com a ata da assembleia que o aprovou; c) regimento dos fundos instituídos pelos cooperados, com a ata da assembleia; d) editais de convocação das três últimas assembleias gerais extraordinárias; e) três registros de presença dos cooperados que executarão o contrato em assembleias gerais ou nas reuniões seccionais; e f) ata da sessão que os cooperados autorizaram a cooperativa a contratar o objeto da licitação;

10.3.2.7. A última auditoria contábil-financeira da cooperativa, conforme dispõe o art. 112 da Lei nº 5.764/1971, ou uma declaração, sob as penas da lei, de que tal auditoria não foi exigida pelo órgão fiscalizador.

10.4. **Habilitações fiscal, social e trabalhista**

10.4.1. As habilitações fiscal, social e trabalhista serão aferidas mediante a verificação dos seguintes requisitos, conforme disposto no art. 68 da Lei nº 14.133/2021:

10.4.1.1. A inscrição no Cadastro de Pessoas Físicas (CPF) ou no Cadastro Nacional da Pessoa Jurídica (CNPJ);

10.4.1.2. A inscrição no cadastro de contribuintes estadual e/ou municipal, se houver, relativo ao

domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

10.4.1.3. A regularidade perante a fazenda federal, estadual e/ou municipal do domicílio ou sede do licitante, ou outra equivalente, na forma da lei;

10.4.1.4. A regularidade relativa à seguridade social e ao FGTS, que demonstre cumprimento dos encargos sociais instituídos por lei;

10.4.1.5. A regularidade perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452/1943;

10.4.1.6. O cumprimento do disposto no inciso XXXIII do art. 7º da Constituição Federal.

10.4.2. Caso o licitante seja considerado isento dos tributos estaduais e/ou municipais relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.

10.4.3. O licitante enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar nº 123/2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal, uma vez que o certificado de microempreendedor -CCMEI, supre as exigências de inscrição nos cadastros fiscais, na medida em que essas informações constam no próprio certificado.

10.4.4. Os documentos enumerados no subitem 10.5.1, poderão ser substituídos ou supridos, no todo ou em parte, por outros meios hábeis a comprovar a regularidade do licitante, inclusive por meio eletrônico. Quanto a comprovação de atendimento do disposto nos subitens 10.4.1.3, 10.4.1.4 e 10.4.1.5 deverá ser feita na forma da legislação específica.

10.4.5. Para os Estados e Municípios que emitam prova de regularidade fiscal em separado, os proponentes deverão apresentar as respectivas certidões.

10.4.6. Os documentos relativos à regularidade fiscal somente serão exigidos, em qualquer caso, em momento posterior ao julgamento das propostas, e apenas do licitante melhor classificado.

10.4.6.1. Respeitada a exceção do subitem anterior, relativa à regularidade fiscal, quando a fase de habilitação anteceder as fases de apresentação de propostas e lances e de julgamento, a verificação ou exigência do presente subitem ocorrerá em relação a todos os licitantes.

10.5. **Habilitação econômico-financeira**

10.5.1. A habilitação econômica financeira será aferida mediante a apresentação da seguinte documentação, nos termos do art. 69 da Lei nº 14.133/2021:

10.5.1.1. Certidão negativa de feitos sobre falência expedida pelo distribuidor da sede do licitante, exceto as sociedades cooperativas, conforme dispõe o art. 4º da Lei nº 5.764/71. No caso de pessoa física ou de socie-dade simples, certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede do licitante.

10.5.1.1.1. Na ausência da certidão negativa, o licitante em recuperação judicial deverá comprovar o acolhi-mento judicial do plano de recuperação judicial nos termos do art. 58 da Lei nº 11.101/2005. No caso do licitante em recuperação extrajudicial deverá apresentar a homologação judicial do plano de recuperação.

10.6. Os documentos de habilitação deverão ser apresentados ou pela matriz ou pela filial que estiver participando do certame, com exceção dos documentos que são válidos tanto para matriz como para as filiais como é o caso dos atestados de capacidade técnica. O contrato será celebrado com a sede que apresentou a documentação.

10.7. O documento obtido através de sítios oficiais, que esteja condicionado à aceitação via internet, terá sua autenticidade verificada pelo pregoeiro.

10.7.1. Os documentos têm que se encontrar dentro do prazo de validade. Na hipótese de o documento não constar expressamente a validade, este deverá ser acompanhado de declaração ou regulamentação do órgão emissor que disponha sobre sua validade. Na ausência de tal declaração ou regulamentação, o documento será considerado válido pelo prazo de 90 (noventa) dias, contados a partir da data de sua emissão, quando se tratar de documentos referentes à habilitação fiscal e econômico-financeira.

11. DA APRESENTAÇÃO DA PROPOSTA ELETRÔNICA E DOS DOCUMENTOS DE HABILITAÇÃO

11.1. Na presente licitação, a fase de habilitação sucederá as fases de apresentação de propostas e lances e de julgamento.

11.1.1. Os licitantes encaminharão, exclusivamente por meio do sistema eletrônico, a proposta com o preço ou o percentual de desconto, conforme o critério de julgamento adotado neste edital, até a data e o horário estabelecidos para abertura da sessão pública.

11.1.2. **A licitante deverá fornecer junto com a proposta de preços:**

11.1.2.1 Descrição detalhada das características técnicas dos itens cotados, que permitam uma avaliação completa e precisa dos mesmos.

11.1.2.2 O **ANEXO E – COMPROVAÇÃO DAS ESPECIFICAÇÕES TÉCNICAS**, parte integrante do **ANEXO I – Termo de Referência**, é de preenchimento obrigatório pela Licitante, sendo motivo de desclassificação do certame o seu não preenchimento.

11.1.2.2.1 O **ANEXO E** deverá ser apresentado preenchido e acompanhado de todas as comprovações dos requisitos exigidos no item **1.1, ESPECIFICAÇÃO DETALHADA** do **ANEXO A – ESPECIFICAÇÕES DETALHADAS**, assim como no **ANEXO B - ESPECIFICAÇÕES DA SOLUÇÃO DE GERÊNCIA CENTRALIZADA E RELATORIA** e no **ANEXO C - PLATAFORMA DE MONITORAMENTO**, incluindo, mas não se limitando a: catálogos, manuais, declaração, ficha de especificação técnica e/ou informações obtidas em sites oficiais do fabricante através da Internet

11.1.3. No VALOR UNITÁRIO dos itens deve ser informado o valor total a ser pago durante toda a execução do contrato, cujo prazo é de 12 (doze) meses para os itens 1 a 28, e de 36 (trinta e seis meses) para os itens 29 a 35.

11.2. Após o julgamento da proposta, o licitante vencedor deverá enviar, no prazo máximo de 24 (vinte e quatro) horas a contar da convocação do pregoeiro, todos os documentos de habilitação.

11.3. Para efeito de julgamento das propostas eletrônicas, o valor a ser informado no sistema eletrônico, pelos licitantes situados no Estado do Ceará, será o valor deduzido do percentual de 7,5% (sete inteiros e cinco décimos por cento), correspondente à média das diferenças de alíquotas interestaduais do ICMS, nos termos do disposto no Decreto Estadual nº 27.624/2004.

11.3.1. A dedução acima referida não se aplica ao fornecimento de produtos isentos e não tributados, e, na hipótese de a alíquota interna ser inferior ao percentual de 7,5% (sete inteiros e cinco décimos por cento), devendo neste caso, ser aplicado o percentual correspondente à alíquota cobrada.

11.4. Após a entrega dos documentos para habilitação e/ou proposta, não será permitida a substituição ou a apresentação de novos documentos, salvo em sede de diligência conforme art. 64 da Lei nº 14.133/21. O licitante deverá enviar os documentos complementares via sistema no prazo de 24 (vinte e quatro) horas a contar da solicitação.

11.4.1 Não se caracterizam documentos novos aqueles que venham a comprovar fatos existentes à época da abertura da sessão, com respaldo no previsto no Acórdão 1211/2021-TCU-Plenário.

11.4.2. Realizada a diligência, o não envio das informações ou documentos no prazo estabelecido pelo pregoeiro, ensejará a preclusão desse direito, resultando na inabilitação e/ou desclassifica-

ção do licitante.

11.5. A não apresentação de autodeclarações formais e/ou termos de compromissos exigidos, exceto a declaração de que sua proposta compreende a integralidade dos custos para atendimento dos direitos trabalhistas conforme subitem 11.6.1, não implicarão na desclassificação ou inabilitação imediata do licitante. Compete a Administração mediante diligência, conceder o mesmo prazo estabelecido no subitem 11.4 para o devido saneamento, em respeito aos princípios do formalismo moderado e da razoabilidade.

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

11.6.1. Está ciente e concorda com as condições contidas no edital e seus anexos, bem como de que a proposta apresentada compreende a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de condutas vigentes na data de sua entrega em definitivo e que cumpre plenamente os requisitos de habilitação definidos no instrumento convocatório;

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

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

11.6.4. Cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da previdência social ou para aprendiz, bem como as reservas de cargo previstas em lei e em outras normas específicas, conforme disposto no art. 116 da Lei nº 14.133/2021;

11.6.5. O licitante enquadrado como microempresa, empresa de pequeno porte ou a sociedade cooperativa que cumpra os requisitos estabelecidos no art. 16 da Lei nº 14.133/2021, deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no art. 3° da Lei Complementar nº 123/2006, estando apto a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49, observado o disposto nos §§ 1º ao 3º do art. 4º, da Lei nº 14.133/2021;

11.6.5.1. 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;

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

11.7. A falsidade das declarações de que tratam os subitens 11.6.1 ao 11.6.5, sujeitará o licitante às sanções previstas na Lei Federal nº 14.133/2021, e neste edital.

11.8. Os licitantes poderão retirar ou substituir as propostas no sistema, até a abertura da sessão pública.

11.9. 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.

12. DO PREENCHIMENTO DA PROPOSTA

12.1. O licitante deverá enviar sua proposta eletrônica com o preenchimento obrigatório de todos os campos solicitados no sistema.

12.1.1. Os preços globais deverão ser expressos em reais, com até 2 (duas) casas decimais.

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

12.3. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, traba-lhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na execução do objeto.

12.4. Os preços ofertados, tanto na proposta eletrônica, 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.

12.5. Se o regime tributário da empresa implicar o recolhimento de tributos em percentuais variáveis, a cotação adequada será a que corresponde à média dos efetivos recolhimentos da empresa nos últimos doze meses.

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

12.7. A apresentação das propostas implica obrigatoriedade do cumprimento das disposições nelas contidas, assumindo o proponente o compromisso de executar o objeto licitado nos seus termos, e quando for o caso, de fornecer os materiais, equipamentos, ferramentas e utensílios necessários em quantidades e qualidades adequadas à perfeita execução contratual.

12.8. O prazo de validade da proposta não será inferior a 90 (noventa) dias, a contar da data de sua apresentação.

12.9. Os licitantes devem respeitar os preços máximos estabelecidos pela Administração.

12.10. O descumprimento das regras supramencionadas pela Administração por parte dos contratados pode ensejar a responsabilização pelos Tribunais de Contas e, após o devido processo legal, gerar as seguintes consequências: assinatura de prazo para a adoção das medidas necessárias ao exato cumprimento da lei, ou condenação dos agentes públicos responsáveis e do contratado ao pagamento dos prejuízos ao erário, caso verificada a ocorrência de superfaturamento ou sobrepreço na execução do contrato.

13. DA ABERTURA DA SESSÃO, CLASSIFICAÇÃO DAS PROPOSTAS E FORMULAÇÃO DE LANCES

13.1. A abertura da presente licitação dar-se-á automaticamente em sessão pública, por meio de sistema eletrônico, na data, horário e local indicados neste edital, vedada a identificação do licitante, sob pena de desclassificação.

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

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

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

13.3. O sistema disponibilizará campo próprio para troca de mensagens entre o pregoeiro e os licitantes.

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

13.5. O lance deverá ser ofertado pelo valor unitário.

13.6. Os licitantes poderão oferecer lances sucessivos, observando o horário fixado para abertura da sessão e as regras estabelecidas neste edital.

13.7. O licitante poderá, uma única vez, excluir seu último lance ofertado, no intervalo de quinze

segundos após o registro no sistema, na hipótese de lance inconsistente ou inexequível.

13.8. Os licitantes somente poderão oferecer lances de valor unitário inferior ao último por eles ofertados e registrados pelo sistema.

13.9. O intervalo mínimo de diferença de valores entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser de 0,2% (dois décimos por cento), utilizando como referência o valor unitário do item.

13.10. 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:

13.10.1. 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

13.10.2. Os lances serão de envio automático pelo sistema, respeitado o valor final mínimo ou percentual estabelecido e o intervalo de que trata o subitem acima.

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

13.11.1. Valor superior a lance já registrado por ele mesmo no sistema, quando adotado o critério de julgamento por menor preço; e

13.12. O valor final mínimo parametrizado na forma do subitem 13.11 possuirá caráter sigiloso para os demais licitantes e para o pregoeiro, podendo ser disponibilizado estrita e permanentemente aos órgãos de controle externo e interno.

13.13. No modo de disputa "**aberto e fechado**" os licitantes apresentarão lances públicos e sucessivos, com lance final e fechado.

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

13.13.2. Encerrado o prazo previsto no subitem anterior, o sistema abrirá oportunidade para que o autor da melhor oferta e os das ofertas com preços até 10% (dez por cento) superiores) àquela, possam ofertar um lance final e fechado em até cinco minutos, o qual será sigiloso até o encerramento deste prazo.

13.13.3. O licitante poderá optar por manter o seu último lance da etapa aberta, ou por ofertar melhor lance.

13.13.4. Não havendo pelo menos três ofertas nas condições definidas no subitem 13.13.2, poderão os autores dos melhores lances subsequentes, na ordem de classificação, até o máximo de três, oferecer um lance final e fechado em até cinco minutos, o qual será sigiloso até o encerramento deste prazo, observado o disposto no subitem 13.13.3.

13.13.5. Poderá o pregoeiro, auxiliado pela equipe de apoio, justificadamente, admitir o reinício da etapa fe-chada, caso nenhuma licitante classificada na etapa de lance fechado atender às exigências de habilitação.

13.13.6. Após o término dos prazos estabelecidos nos subitens anteriores, o sistema ordenará e divulgará os lances segundo a ordem crescente.

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

13.15. Durante o transcurso da sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado, vedada a identificação do licitante. O sistema não identificará o autor dos lances ao pregoeiro nem aos demais participantes.

13.16. No caso de desconexão com o pregoeiro, no decorrer da etapa competitiva do pregão, o sistema ele-trônico poderá permanecer acessível aos licitantes para a recepção dos lances, sem prejuízos dos atos realizados.

13.17. Quando a desconexão do sistema eletrônico para o pregoeiro persistir por tempo superior a dez minutos, a sessão pública será suspensa e reiniciada somente após decorridas 24 (vinte e quatro) horas da comunicação do fato pelo pregoeiro aos participantes, no sítio eletrônico utilizado para divulgação.

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

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

13.19.1. Em caso de empate entre duas ou mais propostas ou lances, serão utilizados os seguintes critérios de desempate, nesta ordem:

13.19.1.1. Disputa final, hipótese em que os licitantes empatados poderão apresentar nova proposta ou lance em ato contínuo à classificação;

13.19.1.2. Avaliação do desempenho contratual prévio dos licitantes, para a qual deverão preferencialmente ser utilizados registros cadastrais para efeito de atesto de cumprimento de obrigações previstos na Lei Federal nº 14.133/2021;

13.19.1.3. Desenvolvimento pelo licitante de ações de equidade entre homens e mulheres no ambiente de trabalho, conforme regulamento;

13.19.1.4. Desenvolvimento pelo licitante de programa de integridade, conforme orientações dos órgãos de controle.

13.19.2. Em igualdade de condições, se não houver desempate, será assegurada preferência, sucessivamente, aos bens e serviços produzidos ou prestados por:

13.19.2.1. Empresas estabelecidas no território do Estado do Ceará;

13.19.2.2. Empresas brasileiras;

13.19.2.3. Empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País;

13.19.2.4. Empresas que comprovem a prática de mitigação, nos termos da Lei nº 12.187/2009.

13.19.3. Esgotados todos os critérios de desempate previstos em lei, a escolha do licitante vencedor ocorrerá por sorteio, em ato público, para o qual todos os licitantes empatados serão convocados, vedado qualquer outro processo.

13.19.3.1. Será comunicado, por meio do sistema, a data, o horário, o sítio eletrônico onde será realizado o sorteio, bem como a plataforma de transmissão ao vivo;

13.19.3.2. A data e o horário serão comunicados no prazo de 24 (vinte e quatro) horas que antecedem a realização do sorteio;

13.19.3.3. O resultado do sorteio será registrado na ata da sessão pública, divulgado a todos os licitantes e anexado aos autos do processo licitatório.

13.20. Encerrada a etapa de envio de lances da sessão pública, o pregoeiro deverá negociar condições mais vantajosas com o primeiro colocado, vedada a negociação em condições diferentes das previstas neste edital.

13.20.1. A negociação deverá ser feita com os demais licitantes, segundo a ordem de classificação inicialmente estabelecida, quando o primeiro colocado, mesmo após a negociação, for desclassificado em razão de sua proposta permanecer acima do preço máximo definido pela Administração.

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

13.20.3. O resultado da negociação será divulgado a todos os licitantes e anexado aos autos do processo licitatório.

13.20.4. A proposta deverá conter todas as especificações do objeto em atendimento ao Anexo I – Termo de Referência.

13.20.5. O pregoeiro solicitará ao licitante mais bem classificado para no prazo de 24 (vinte e quatro) horas, após a negociação realizada, anexar a proposta adequada ao último lance por ele ofertado.

13.21. Nos termos do Decreto Estadual nº 27.624/2004, o licitante melhor classificado situado no Estado do Ceará deverá apresentar a proposta com o valor acrescido do diferencial referido no subitem 11.3, mediante a utilização da seguinte fórmula:

$$VFP = \frac{VPV}{0,925}$$; Onde:

VFP = Valor Final da Proposta, acrescido da alíquota de 7,5% (sete inteiros e cinco décimos por cento);

VPV = Valor da Proposta Vencedora após o encerramento da disputa eletrônica anunciado pelo sistema;

0,925 = Fator de Reversão correspondente a 7,5% (sete inteiros e cinco décimos por cento), que foram deduzidos antes da disputa.

14. DA FASE DE JULGAMENTO

14.1. Encerrada a etapa de negociação, o pregoeiro verificará se o licitante provisoriamente classificado em primeiro lugar atende às condições de participação no certame, observado o previsto no art. 14 da Lei nº 14.133/21, legislação correlata e no subitem 8.1, deste edital, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

I- Sistema de Cadastramento Unificado de Fornecedores(SICAF);

II- Certificado de Registro Cadastral(CRC)CE.

III- Cadastro Nacional de Empresas Inidôneas e Suspensas(CEIS), mantido pela Controladoria-Geral da União (https://www.portaltransparencia.gov.br/sancoes); e

IV- Cadastro Nacional de Empresas Punidas(CNEP), mantido pela Controladoria-Geral da União (https://www.portaltransparencia.gov.br/sancoes).

14.2. A consulta aos cadastros será realizada em nome da empresa licitante.

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

14.4. 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 presente edital, observado o prazo disposto no subitem 13.21.5 deste edital.

14.4.1. As decisões do pregoeiro se darão baseadas nos pareceres e laudos, nos termos previstos no subitem 9.2.1, deste edital.

14.4.2. Somente serão disponibilizados para acesso público os documentos de habilitação do licitante cuja proposta atenda ao edital de licitação, após concluídos os procedimentos de que trata o subitem anterior.

14.5. Caso o licitante provisoriamente classificado em primeiro lugar tenha se utilizado de algum

tratamento favorecido às ME/EPPs, o pregoeiro verificará se faz jus ao referido benefício.

14.6. 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 ao máximo estipulado para contratação neste edital e em seus anexos.

14.7. **Será desclassificada a proposta vencedora que**:

14.7.1. Contiver vícios insanáveis;

14.7.2. Não obedecer às especificações técnicas contidas no termo de referência;

14.7.3. Apresentar preços inexequíveis ou permanecer acima do preço máximo definido para a contratação;

14.7.4. Não tiver sua exequibilidade demonstrada, quando exigido pela Administração;

14.7.5. Apresentar desconformidade com quaisquer outras exigências deste edital ou seus anexos, desde que insanável;

14.7.6. Deixar de apresentar a declaração de que sua proposta compreende a integralidade dos custos para atendimento dos direitos trabalhistas conforme subitem 11.6.1 deste edital.

14.8. Quando houver agrupamento de itens, a proposta final para o grupo não poderá conter item com valor superior ao estimado pela administração, sob pena de desclassificação, independentemente do valor total do grupo.

14.9. A ausência de documentos possíveis de ser verificados em sites oficiais, não é motivo de desclassificação.

14.10. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, para que o licitante comprove a exequibilidade da proposta, conforme disposto no inciso IV do art. 59 da Lei nº 14.133/2021.

15. DOS RECURSOS

15.1. 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 14.133/2021.

15.2. O prazo recursal é de 3 (três) dias úteis, contados da data de intimação ou de lavratura da ata de julgamento da proposta, ou da habilitação ou inabilitação.

15.3. Quando a decisão do pregoeiro importar em abertura de prazo recursal, será comunicada a retomada da sessão pública com, no mínimo, 24 (vinte e quatro) horas de antecedência, no sítio eletrônico utilizado para realização do certame.

15.3.1. Qualquer licitante poderá, durante o prazo de 10 (dez) minutos, de forma imediata após o 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.

15.4. Os recursos deverão ser encaminhados em campo próprio do sistema.

15.5. O recurso será dirigido à autoridade que tiver editado o ato ou proferido a decisão recorrida, a qual poderá reconsiderar sua decisão no prazo de 3 (três) dias úteis, ou, nesse mesmo prazo, encaminhar recurso para a autoridade superior, a qual deverá proferir sua decisão no prazo de 10 (dez) dias úteis, contado do recebimento dos autos.

15.6. Os recursos interpostos fora do prazo não serão conhecidos.

15.7. O prazo para apresentação de contrarrazões ao recurso pelos demais licitantes será de 3 (três) dias úteis, contados da data da intimação pessoal ou da divulgação da interposição do

recurso, assegurada a vista imediata dos elementos indispensáveis à defesa de seus interesses.

15.7.1. Caso o licitante entenda ser necessário o envio de documentos complementares para melhor entendimento das suas razões e/ou contrarrazões de recurso, deverá disponibilizar um link no corpo da peça, de maneira que os referidos documentos sejam de acesso livre ao pregoeiro e demais interessados.

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

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

15.10. Não serão conhecidos os recursos intempestivos e/ou subscritos por representante não habilitado legalmente ou não identificado no processo licitatório para responder pelo proponente.

15.11. Os autos do processo permanecerão com vista franqueada aos interessados no Portal Nacional de Contratações Públicas (PNCP), naquilo que lhes couber e na Central de Licitações no endereço constante no subitem 7.1 deste edital.

16. DA HOMOLOGAÇÃO E DA ASSINATURA DA ATA DE REGISTRO DE PREÇOS

16.1. O sistema gerará ata circunstanciada, na qual estarão registrados todos os atos do procedimento e as ocorrências relevantes.

16.2. Para efeito de homologação da licitação, o registro de preços observará, entre outras, as condições previstas no art. 11 do Decreto nº 35.323/2023, inclusive em relação a formação do cadastro reserva e demais licitantes classificados na licitação.

16.3. Após a homologação do resultado da licitação, os preços ofertados pelos licitantes vencedores dos itens, serão registrados na Ata de Registro de Preços, elaborada conforme o anexo III deste edital, pelo valor unitário do item.

16.4. Os licitantes classificados em primeiro lugar terão o prazo de 5 (cinco) dias úteis, a contar da data do recebimento da convocação, para comparecerem perante o gestor a fim de assinarem a Ata de Registro de Preços, sob pena de decair do direito à contratação, e sem prejuízo das sanções previstas no edital, podendo o prazo de comparecimento ser prorrogado uma vez, por igual período, desde que ocorra motivo justificado e aceito pela administração.

16.5. A Ata de Registro de Preços poderá ser assinada por certificação digital, com autenticidade reconhecida pelo ICP-Brasil.

16.6. A habilitação dos licitantes que comporão o cadastro de reserva e dos demais classificados da licitação será julgada pelo pregoeiro, conforme §3º do art. 11 do Decreto nº 35.323/2023.

16.7. A cota para participação exclusiva terá prioridade de contratação, ressalvados os casos em que for inadequada para atender às quantidades ou as condições do pedido, justificadamente, conforme disposto no art. 8º, §7º do Decreto 35.323/2023.

17. DA ATA DE REGISTRO DE PREÇOS

17.1. A Empresa da Tecnologia da Informação do Ceará – ETICE será o órgão gestor da Ata de Registro de Preços de que trata este edital.

17.2. A Ata de Registro de Preços, elaborada conforme anexo III, será assinada pelo titular da ETICE, órgão gestor do Registro de Preços ou, por delegação, por seu substituto legal, e pelos representantes de cada um dos licitantes legalmente credenciados e identificados.

17.2.1. O prazo de vigência da Ata de Registro de Preços será de 1 (um) ano, contado a partir da data da sua publicação no Diário Oficial do Estado, e poderá ser prorrogado, por igual período, desde que por acordo en-tre as partes e comprovado o preço vantajoso, nas mesmas condições e quantidades ou valores remanescentes.

17.3. Os preços registrados na Ata de Registro de Preços serão divulgados no Portal de Compras

do Estado e no Portal Nacional de Contratações Públicas (PNCP), e ficarão disponibilizados, por, no mínimo, a vigência da ata de registro de preços.

17.4. A Ata de Registro de Preços uma vez lavrada e assinada, não obriga a Administração a firmar as contra-tações que dela poderão advir, ficando-lhe facultada a utilização de licitação específica, desde que devida-mente motivada, sendo assegurado ao detentor do registro de preços a preferência em igualdade de condições.

17.5. O participante do SRP (Sistema de Registro de Preços), quando necessitar, efetuará contratações junto aos detentores de preços registrados, de acordo com os quantitativos e especificações previstos, durante a vigência do Ata.

17.6. Os detentores de preços registrados ficarão obrigados a fornecer o objeto licitado aos órgãos e entidades participantes do SRP (Sistema de Registro de Preços), nos prazos, quantidades e demais condições definidas no Anexo I – Termo de Referência deste edital.

17.7. A Ata de Registro de Preços, durante sua vigência, poderá ser utilizada por órgão ou entidade de outros entes federativos, como órgãos e entidades interessados, mediante consulta prévia ao órgão gestor do registro de preços, conforme disciplina o art. 20 do Decreto nº 35.323/2023.

17.8. Os órgãos e entidades interessados, quando desejarem fazer uso da Ata de Registro de Preços, deverão manifestar seu interesse junto ao órgão gestor do Registro de Preços, o qual indicará o fornecedor de serviço e o preço a ser praticado.

17.8.1. As contratações decorrentes da utilização da Ata de Registro de Preços de que trata este subitem não poderão exceder, por órgão e entidades interessados, a 50% (cinquenta por cento) dos quantitativos dos itens do instrumento convocatório registrados na ata de registro de preços para o órgão gerenciador e para os órgãos participantes.

17.8.2. O quantitativo decorrente das adesões à Ata de Registro de Preços a que se refere o subitem anterior, não poderá exceder, na totalidade, ao dobro do quantitativo de cada item registrado na ata de registro de preços para o órgão gerenciador e órgãos participantes, independentemente do número de órgãos e entidades interessados que aderirem.

17.8.3. Os órgãos e entidades interessados deverão efetivar a contratação em até 90 (noventa) dias, con-tados a partir da autorização do órgão gestor do registro de preços, observado o prazo de vigência da ata.

17.8.4. A comunicação ao gestor do registro de preços acerca do cumprimento do prazo previsto no subitem 17.8.3. Será providenciada pelo órgão e entidades interessados até o quinto dia útil após a contratação.

17.8.5. A entidade gestora do registro de preços não autorizará a adesão à ata de registro de preços para contratação separada de itens de objeto adjudicado por preço global para os quais o detentor do registro não tenha apresentado o menor preço.

17.9. Caberá à entidade gestora do Registro de Preços, para utilização da Ata por órgãos e entidades interessados da Administração Pública, proceder a indicação do licitante detentor do preço registrado, obedecida à ordem de classificação.

17.10. O detentor de preços registrados que descumprir as condições da Ata de Registro de Preços, terá o seu registro cancelado nas hipóteses previstas nos incisos I a IX do art. 25 do Decreto n° 35.323/2023.

17.11. Os preços registrados poderão ser revistos a qualquer tempo em decorrência da redução dos preços praticados no mercado ou de fato que eleve os custos dos itens registrados, observado o constante no art. 23 do Decreto nº 35.323/2023.

17.12. A entidade gestora convocará o detentor do preço registrado para negociar o preço e adequá-lo ao preço de mercado, sempre que verificar que o preço registrado está acima do preço

de mercado.

17.12.1. Não havendo êxito nas negociações, o gestor da Ata poderá convocar os demais licitantes classificados, podendo negociar os preços de mercado, ou cancelar o item, ou ainda revogar a Ata de Registro de Preços.

17.13. Serão considerados preços de mercado, os preços que forem iguais ou inferiores à média daqueles apurados pela Administração para os itens registrados.

17.14. O detentor do item registrado poderá solicitar a substituição da marca ou modelo registrados na ata por outra equivalente ou de qualidade superior, mantendo o mesmo preço e a mesma especificação, nos termos do art. 24, do Decreto n.º 35.323/2023.

17.15. As alterações registradas, oriundas de revisão dos preços ou da marca ou modelo do item registrado, serão publicadas no Diário Oficial do Estado e na página oficial do Governo do Estado na internet.

17.16. As demais condições contratuais se encontram estabelecidas no Anexo I – Termo de Referência e IV – Minuta do Termo de Contrato, parte integrante deste Edital.

17.17. As quantidades previstas no Anexo I – Termo de Referência deste edital, são estimativas máximas para o período de validade da Ata de Registro de Preços, reservando-se a Administração, através do órgão e entidade participante, o direito de adquirir o quantitativo que julgar necessário ou mesmo abster-se de adquirir o item especificado.

18. DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES

18.1. Comete infração administrativa, nos termos do art. 155 da Lei nº 14.133/2021, o licitante que, com dolo ou culpa:

18.1.1. Deixar de entregar a documentação exigida para o certame ou não entregar qualquer documento que tenha sido solicitado pelo pregoeiro durante o certame;

18.1.2. Salvo em decorrência de fato superveniente devidamente justificado, não mantiver a proposta em especial quando:

18.1.2.1. Não enviar a proposta adequada ao último lance ofertado ou após a negociação;

18.1.2.2. Recusar-se a enviar o detalhamento da proposta quando exigível;

18.1.2.3. Pedir para ser desclassificado quando encerrada a etapa competitiva ou;

18.1.2.4. Apresentar proposta em desacordo com as especificações do edital;

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

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

18.1.4. Apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação;

18.1.5. Fraudar a licitação;

18.1.6. Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza, em especial quando:

18.1.6.1. Agir em conluio ou em desconformidade com a lei;

18.1.6.2. Induzir deliberadamente a erro no julgamento;

18.1.7. Praticar atos ilícitos com vistas a frustrar os objetivos da licitação;

18.1.8. Praticar ato lesivo previsto no art. 5º da Lei nº 12.846/2013.

18.2. Com fulcro na Lei nº 14.133/2021, a Administração poderá, garantida a prévia defesa,

aplicar aos licitantes e/ou adjudicatários as seguintes sanções, sem prejuízo das responsabilidades civil e criminal:

18.2.1. Advertência;

18.2.2. Multa;

18.2.3. Impedimento de licitar e contratar e

18.2.4. 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;

18.3. Na aplicação das sanções serão considerados:

18.3.1. A natureza e a gravidade da infração cometida;

18.3.2. As peculiaridades do caso concreto;

18.3.3. As circunstâncias agravantes ou atenuantes;

18.3.4. Os danos que dela provierem para a Administração Pública;

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

18.4. A sanção de multa não poderá ser inferior a 0,5% (cinco décimos por cento) nem superior a 30% (trinta por cento) do valor do contrato licitado, conforme §3º do art. 156 da Lei nº 14.133/2021.

18.4.1. A multa será recolhida no prazo máximo de 20 (vinte) dias úteis, a contar da comunicação oficial.

18.4.1.1. Para as infrações previstas nos subitens 18.1.1, 18.1.2 e 18.1.3, a multa será de 10% (dez por cento) do valor do contrato licitado.

18.4.1.2. Para as infrações previstas nos subitens 18.1.4, 18.1.5, 18.1.6, 18.1.7 e 18.1.8, a multa será de 15% (quinze por cento) do valor do contrato licitado.

18.5. As sanções de advertência, impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar poderão ser aplicadas, cumulativamente ou não, à penalidade de multa.

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

18.7. A sanção de impedimento de licitar e contratar será aplicada ao responsável em decorrência das infrações administrativas relacionadas nos subitens 18.1.1, 18.1.2 e 18.1.3, 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.

18.8. Poderá ser aplicada ao responsável a sanção de declaração de inidoneidade para licitar ou contratar, em decorrência da prática das infrações dispostas nos subitens 18.1.4, 18.1.5, 18.1.6, 18.1.7 e 18.1.8, bem como pelas infrações administrativas previstas nos subitens 18.1.1, 18.1.2 e 18.1.3 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 n.º 14.133/2021.

18.9. A recusa injustificada do adjudicatário em assinar o contrato, ou em aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração, descrita no subitem 18.1.3, caracterizará o descumprimento total da obrigação assumida e o sujeitará às penalidades e à imediata perda da garantia de proposta, se houver, em favor do órgão ou entidade promotora da licitação.

18.9.1. A exigência da garantia de que trata o subitem anterior, obedecerá o disposto no art. 58 da

Lei Federal nº 14.133/2021.

18.10. O licitante recolherá a multa por meio de Documento de Arrecadação Estadual (DAE), podendo ser substituído por outro instrumento legal, em nome do órgão contratante, se não o fizer, será cobrada em processo de execução

19. DA ESTIMATIVA DO VALOR DA CONTRATAÇÃO

19.1. O custo estimado total da contratação possui caráter sigiloso e será tornado público apenas e imediatamente após o julgamento das propostas.

20. DA ADJUDICAÇÃO E DA HOMOLOGAÇÃO

20.1. A adjudicação do objeto e a homologação da licitação é de responsabilidade da autoridade superior.

20.2. O sistema gerará o relatório de disputa e de adjudicação e homologação.

21. DA CONTRATAÇÃO

21.1. O adjudicatário terá o prazo de 5 (cinco) dias úteis, contados a partir da convocação, para a assinatura do contrato. Este prazo poderá ser prorrogado uma vez por igual período, desde que solicitado durante o seu transcurso e, ainda assim, se devidamente justificado e aceito.

21.2. O contrato poderá ser assinado por certificação digital, com autenticidade reconhecida pelo ICP-Brasil.

21.3. Na assinatura do contrato será exigida a comprovação das condições de habilitação exigidas neste edital, as quais deverão ser mantidas pelo contratado durante todo o período da contratação, bem como a apresentação do Certificado de Registro Cadastral – CRC, emitido pela Secretaria de Planejamento e Gestão do Estado do Ceará.

21.4. Quando o adjudicatário não comprovar as condições habilitatórias consignadas neste edital, ou recusar-se a assinar o contrato, poderá ser convidado outro licitante pelo pregoeiro, desde que respeitada a ordem de classificação, para, depois de comprovados os requisitos habilitatórios e feita a negociação, assinar o contrato.

21.5. A forma de pagamento, prazo contratual, obrigações, reajuste, recebimento e demais condições aplicáveis à contratação estão definidas respectivamente nos Anexos I e IV – Termo de Referência e Minuta do Termo de Contrato, parte integrante deste edital.

21.6. Da Garantia

21.6.1. Será exigida garantia contratual nos termos e prazos estabelecidos na cláusula décima segunda da minuta do contrato. A não prestação de garantia equivale à recusa injustificada para a contratação, caracterizando descumprimento total da obrigação assumida, ficando a adjudicatária sujeita às penalidades legalmente estabelecidas, inclusive multa.

21.6.2. Adotada a modalidade seguro-garantia, prevista no inciso II do § 1º do art. 96 da Lei nº 14.133/2021, o licitante deverá apresentá-la no valor correspondente a 5% (cinco por cento) do valor contratado, no prazo de 1(um) mês, contado da data de homologação da licitação e anterior à assinatura do contrato conforme § 3º do mesmo artigo suprarreferido.

21.7. **Da Subcontratação**

21.7.1. É permitida a subcontratação parcial do objeto, até o limite de 25% (vinte e cinco por cento) do valor total do contrato.

21.7.1.1. É vedada a subcontratação integral do objeto.

21.7.2. Em qualquer hipótese de subcontratação, permanece a responsabilidade integral do contratado pela perfeita execução contratual, cabendo-lhe realizar a supervisão e coordenação das atividades do subcontratado, bem como responder perante o contratante pelo rigoroso cumprimento das obrigações contratuais correspondentes ao objeto da subcontratação.

21.7.3. A subcontratação depende de autorização prévia do contratante, a quem incumbe avaliar se o subcontratado cumpre os requisitos de qualificação técnica necessários para a execução do objeto.

21.7.4. O contratado apresentará à Administração documentação que comprove a capacidade técnica do subcontratado, que será avaliada e juntada aos autos do processo correspondente.

21.7.5. É vedada a subcontratação de pessoa física ou jurídica, se aquela ou os dirigentes desta mantiverem vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que desempenhe função na contratação ou atue na fiscalização ou na gestão do contrato, ou se deles forem cônjuge, companheiro ou parente em linha reta, colateral, ou por afinidade, até o terceiro grau.

22. DAS DISPOSIÇÕES GERAIS

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

22.2. 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.

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

22.4. Na contagem dos prazos estabelecidos neste edital, excluir-se-ão os dias de início e incluir-se-ão os dias de vencimento. Os prazos estabelecidos neste edital para a fase externa se iniciam e se vencem somente nos dias e horários de expediente da Central de Licitações. Os demais prazos se iniciam e se vencem exclusivamente em dias úteis de expediente do contratante.

22.5. 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.

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

22.7. É facultada ao pregoeiro ou à autoridade competente, em qualquer fase da licitação, a promoção de diligência destinada a esclarecer ou a complementar a instrução do processo licitatório.

22.8. O descumprimento de prazos estabelecidos neste edital e/ou pelo pregoeiro ou o não atendimento às solicitações ensejará DESCLASSIFICAÇÃO ou INABILITAÇÃO do licitante.

22.9. Toda a documentação fará parte dos autos e não será devolvida a licitante, ainda que se trate de originais.

22.10. Os representantes legais dos licitantes são responsáveis pela fidelidade e legitimidade das informações e dos documentos apresentados em qualquer fase da licitação.

22.11. Os casos omissos serão resolvidos pelo pregoeiro, nos termos da legislação pertinente.

22.12. O foro designado para julgamento de quaisquer questões judiciais resultantes deste edital será o da Comarca de Fortaleza, Capital do Estado do Ceará.

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

ANEXO I – Termo de Referência

ANEXO II – Carta Proposta

ANEXO III – Minuta da Ata de Registro de Preços

ANEXO IV A – Minuta do Termo de Contrato

ANEXO IV B – Minuta do Termo de Contrato (Modelo para Estatais)

Fortaleza – CE, 22 de outubro de 2024.

_____

ORDENADOR DE DESPESA

_____

Analisado e aprovado o processo da contratação pela Procuradoria Jurídica

ANEXO I - TERMO DE REFERÊNCIA

Processo n° 30032.000154/2024-71

UNIDADE REQUISITANTE: ETICE

DO OBJETO:

1.1. Registro de preços para futuras e eventuais aquisições de solução de proteção de redes, incluindo aquisições de hardware e software e respectivo serviço de implantação, posterior monitoramento e suporte técnico 24x7x365, contemplando utilização de equipamentos obrigatoriamente todos novos e de primeiro uso, de acordo com as especificações e quantitativos previstos neste Termo.

1.2. Este objeto será realizado através de licitação na modalidade **PREGÃO**, na forma **ELETRÔNICA**, do tipo **MENOR PREÇO**, com a forma de fornecimento parcelada.

2. DAS ESPECIFICAÇÕES E QUANTITATIVOS

Grupo único – Soluções de Firewall			
ITEM	**DESCRIÇÃO**	**UNIDADE**	**QTDE**
1	NEXT GENERATION FIREWALL – UNIDADE TIPO I	UNIDADE	1000
2	NEXT GENERATION FIREWALL – UNIDADE TIPO II	UNIDADE	50
3	NEXT GENERATION FIREWALL – UNIDADE TIPO III	UNIDADE	20
4	NEXT GENERATION FIREWALL – UNIDADE TIPO IV	UNIDADE	10
5	NEXT GENERATION FIREWALL – SEDE TIPO I	UNIDADE	8
6	NEXT GENERATION FIREWALL – SEDE TIPO II	UNIDADE	12
7	NEXT GENERATION FIREWALL – SEDE TIPO III	UNIDADE	8
8	NEXT GENERATION FIREWALL – DATA CENTER TIPO I	UNIDADE	6
9	NEXT GENERATION FIREWALL – DATA CENTER TIPO II	UNIDADE	4
10	NEXT GENERATION FIREWALL – DATA CENTER TIPO III	UNIDADE	4
11	NEXT GENERATION FIREWALL PARA AMBIENTES VIRTUALIZADOS EM NUVEM PRIVADA (1 QUANTIDADE PARA CADA CORE)	UNIDADE	30
12	SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO E RELATÓRIOS PARA ATÉ 5 EQUIPAMENTOS COMPRASNET: UND SERVIÇO TÉCNICO = SERVIÇO	SERVIÇO	8
13	SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO E RELATÓRIOS PARA ATÉ 10 EQUIPAMENTOS	SERVIÇO	6

	COMPRASNET: UND SERVIÇO TÉCNICO = SERVIÇO		
14	SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO E RELATÓRIOS PARA ATÉ 50 EQUIPAMENTOS COMPRASNET: UND SERVIÇO TÉCNICO = SERVIÇO	SERVIÇO	4
15	SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO E RELATÓRIOS PARA ATÉ 150 EQUIPAMENTOS COMPRASNET: UND SERVIÇO TÉCNICO = SERVIÇO	SERVIÇO	4
16	SOLUÇÃO DE NEXT GENERATION ANTI-MALWARE PARA NOTEBOOKS, DESKTOPS E SERVIDORES COMPRASNET: UND SERVIÇO TÉCNICO = SERVIÇO	SERVIÇO	10000
17	SOLUÇÃO DE PREVENÇÃO DE AMEAÇAS PARA DISPOSITIVOS MÓVEIS ANDROID E IOS COMPRASNET: UND SERVIÇO TÉCNICO = SERVIÇO	SERVIÇO	2000
18	SOLUÇÃO DE PREVENÇÃO DE AMEAÇAS E SPAM PARA E-MAIL EM NUVEM – OFFICE 365 E GOOGLE WORKSPACE COMPRASNET: UND SERVIÇO TÉCNICO = SERVIÇO	SERVIÇO	2000
19	FIREWALL DE APLICAÇÃO WEB – WAF - VIRTUAL	UNIDADE	10
20	FIREWALL DE APLICAÇÃO WEB – WAF – DATACENTER TIPO I	UNIDADE	8
21	FIREWALL DE APLICAÇÃO WEB – WAF – DATACENTER TIPO II	UNIDADE	4
22	INSTALAÇÃO FIREWALL UNIDADE ATÉ 100KM COMPRASNET: UND SERVIÇO TÉCNICO = SERVIÇO	SERVIÇO	500
23	INSTALAÇÃO FIREWALL UNIDADE ATÉ 400KM COMPRASNET: UND SERVIÇO TÉCNICO = SERVIÇO	SERVIÇO	300
24	INSTALAÇÃO FIREWALL UNIDADE ACIMA DE 400KM COMPRASNET: UND SERVIÇO TÉCNICO = SERVIÇO	SERVIÇO	300
25	INSTALAÇÃO FIREWALL SEDE COMPRASNET: UND SERVIÇO TÉCNICO = SERVIÇO	SERVIÇO	28
26	INSTALAÇÃO FIREWALL DATA CENTER COMPRASNET: UND SERVIÇO TÉCNICO = SERVIÇO	SERVIÇO	14
27	INSTALAÇÃO FIREWALL DE APLICAÇÃO WEB – WAF – VIRTUAL COMPRASNET: UND SERVIÇO TÉCNICO = SERVIÇO	SERVIÇO	10

28	INSTALAÇÃO FIREWALL DE APLICAÇÃO WEB – WAF – DATACENTER COMPRASNET: UND SERVIÇO TÉCNICO = SERVIÇO	SERVIÇO	12
29	SERVIÇO DE MONITORAMENTO E SUPORTE TECNICO 24X7 DE FIREWALL UNIDADE TIPO 1 E 2 36 MESES COMPRASNET: UND SERVIÇO TÉCNICO = SERVIÇO	SERVIÇO	1050
30	SERVIÇO DE MONITORAMENTO E SUPORTE TECNICO 24X7 DE FIREWALL UNIDADE TIPO 3 E 4 36 MESES COMPRASNET: UND SERVIÇO TÉCNICO = SERVIÇO	SERVIÇO	30
31	SERVIÇO DE MONITORAMENTO E SUPORTE TÉCNICO 24X7 DE FIREWALL SEDE – 36 MESES COMPRASNET: UND SERVIÇO TÉCNICO = SERVIÇO	SERVIÇO	28
32	SERVIÇO DE MONITORAMENTO E SUPORTE TÉCNICO 24X7 DE FIREWALL DATA CENTER – 36 MESES COMPRASNET: UND SERVIÇO TÉCNICO = SERVIÇO	SERVIÇO	14
33	SERVIÇO DE MONITORAMENTO E SUPORTE TÉCNICO 24X7 DE FIREWALL DE APLICAÇÃO WEB – VIRTUAL – 36 MESES COMPRASNET: UND SERVIÇO TÉCNICO = SERVIÇO	SERVIÇO	10
34	SERVIÇO DE MONITORAMENTO E SUPORTE TÉCNICO 24X7 DE FIREWALL DE APLICAÇÃO WEB – DATACENTER – 36 MESES COMPRASNET: UND SERVIÇO TÉCNICO = SERVIÇO	SERVIÇO	12
35	SERVIÇO DE SOC 24X7 COM SIEM – PACOTES DE 200 EPS – 36 MESES COMPRASNET: UND SERVIÇO TÉCNICO = SERVIÇO	SERVIÇO	30

2.1. Havendo divergências entre as especificações deste anexo e as do sistema, prevalecerão as deste anexo.

2.2. O objeto desta contratação não se enquadra como sendo de bem de luxo, conforme Decreto Estadual nº 34.450/2021.

2.3. Os bens objeto desta contratação são caracterizados como comuns nos termos do inciso IV do art. 32 da Lei Federal nº 13.303/2016.

3. DO PRAZO DE VIGÊNCIA E ALTERAÇÃO CONTRATUAL

3.1. O prazo de vigência da Ata de registro de preços será de 1 (um) ano, contado a partir da data da sua publicação no Diário Oficial do Estado, e poderá ser prorrogado, por igual período, desde que por acordo entre as partes e comprovado o preço vantajoso, nas mesmas condições e quantidades ou valores remanescentes.

3.2. O prazo de vigência do contrato é de 36 (trinta e seis) meses, **contado da sua assinatura**, na forma do art. 94 c/c o art. 105 da Lei Federal n° 14.133/2021, e para as empresas públicas e

sociedades de economia mista, o disposto no art. 71 da Lei Federal n° 13.303/2016.

3.3. O contrato poderá ser alterado pela disciplina dos arts. 124 e seguintes da Lei Federal nº 14.133/2021, e para as empresas públicas e sociedades de economia mista, nos casos previstos nos arts. 72 e 81 da Lei Federal n° 13.303/2016 e conforme dispuser o Regulamento Interno de Licitações e Contratos do contratante.

4. DA DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO.

4.1. A missão institucional da Empresa de Tecnologia da Informação do Ceará – ETICE é fortalecer a gestão pública e o desenvolvimento econômico e social, por meio da Tecnologia da Informação e Comunicação (TIC), consoante o disposto do art. 5º do Decreto nº 32.792, publicado no Diário Oficial do Estado de 23 de agosto de 2018.

4.2. De acordo com o Inciso XXIV, do Decreto supracitado, a Etice possui, dentre as suas principais competências, “construir e gerenciar os processos referentes às aquisições/ contratações corporativas de bens e serviços de TIC no âmbito do Governo do Estado do Ceará”.

4.3. Adicionalmente, segundo a Portaria nº 23/2023 da Secretaria do Planejamento e Gestão - SEPLAG, de forma complementar ao Inciso XXIV citado no parágrafo anterior, é também de sua competência “ser órgão gestor de registro de preços para aquisições e serviços de Tecnologia da Informação e Telecomunicações, para atender aos órgãos e entidades do Estado do Ceará”.

4.4. O Sistema de Registro de Preços (SRP) é regulamentado pelo Decreto Estadual nº 35.323 de 24/2/2023, e prevê no seu artigo 3º, § 1º, as seguintes hipóteses para adoção do SRP:

a) Quando, pelas características do bem ou serviço, houver necessidade de contratações permanentes ou frequentes;

b) Quando for conveniente a aquisição de bens com previsão de entregas parceladas ou contratação de serviços remunerados por unidade de medida, por quantidade de horas de serviço ou postos de trabalho, ou em regime de tarefa;

c) Quando for conveniente a aquisição de bens ou a contratação de serviços para atendimento a mais de um órgão ou entidade, ou a programas de governo; ou

d) Quando, pela natureza do objeto, não for possível definir previamente o quantitativo ou valor a ser demandado pela Administração.

4.5. De acordo com o Art. 12 do Decreto Estadual nº 32.792/2018, compete à Diretoria de Tecnologia e Inovação – DITEC, unidade orgânica da Etice, “promover os processos referentes às aquisições/contratações corporativas de bens e serviços de TIC no âmbito do Governo do Estado do Ceará e da Etice”. Este documento baseia-se especialmente nas recomendações para a adoção de Registro de preços, trazendo os seguintes benefícios:

a) Redução da quantidade de processos licitatórios, diminuindo custos, mitigando riscos e otimizando esforços;

b) Maior celeridade no atendimento de demandas governamentais, por reduzir a burocracia das contratações públicas;

c) Melhor planejamento das contratações públicas, visto que uma ARP tem vigência de, pelo menos, 01 (um) ano, com a nova Lei de Licitações será possível ter vigência de 2 (dois) anos para as Atas;

d) As contratações possam ser fracionadas em várias etapas, permitindo associar, por exemplo, à disponibilidade financeira, favorecendo a decisão pela continuidade ou não de um projeto mediante os resultados que vão sendo obtidos com as contratações já realizadas;

e) O mercado percebe que uma ARP estabelece uma estimativa de quantidades elevadas, favorecendo a participação e a competitividade do processo, representando para o Governo uma excelente oportunidade de ganho em escala por conta da expectativa de preços menores, visto

que o fornecedor detentor da ARP tem a possibilidade de vendas em outras esferas de Governo, inclusive em outros Estados.

4.6. A necessidade de contratar soluções de *firewalls* pode ser vista sob várias perspectivas de seguranças e funcionalidade. Aqui estão algumas razões pelas quais uma organização pode optar por contratar um firewall:

4.6.1. Segurança de Rede: Um firewall atua como a primeira linha de defesa contra ameaças externas, como hackers, malware e ataques de negação de serviço (DdoS). Ele monitora o tráfego de entrada e saída da rede, bloqueando ou permitindo com base em regras predefinidas.

4.6.2. Política de Segurança: Empresas geralmente têm políticas de segurança que determinam o que é permitido e o que é proibido dentro de sua rede. Um firewall permite implementar essas políticas, filtrando o tráfego com base em endereços IP, portas, protocolos e outros critérios.

4.6.3. Controle de Acesso: Firewalls podem ser configurados para controlar quem tem acesso a determinados recursos dentro da rede. Isso é útil para proteger dados sensíveis e restringir o acesso a certas áreas da rede apenas a funcionários autorizados.

4.6.4. Prevenção de Intrusões: Além de bloquear tráfego malicioso conhecido, firewalls modernos podem incluir recursos de prevenção de instruções (IPS), que identificam e bloqueiam atividades suspeitas em tempo real.

4.6.5. Monitoramento de Tráfego: Muitos firewalls fornecem recursos de registros e relatórios que permitem ás organizações monitorar o tráfego de rede, identificar padrões de uso, detectar possíveis ameaças e garantir conformidade com regulamentos de segurança.

4.6.6. Segurança de Aplicações: Além de proteger a rede em si, firewalls também podem ser usados para proteger aplicações específicas, como servidores web e servidores de e-mail, contra ataques direcionados.

4.6.7. Conformidade Regulatória: Em muitas indústrias, há regulamentos específicos de segurança que as empresas devem cumprir. Um firewall pode ser uma parte essencial do cumprimento desses requisitos.

4.6.8. Em resumo, contratar um firewall é essencial para proteger uma rede contra ameaças cibernéticas, garantir a conformidade regulatória e manter a integridade e a segurança dos dados da organização.

A presente justificativa visa embasar a necessidade e os benefícios da implementação de uma ata de registro de preços para a contratação de futuras e eventuais aquisições de solução de proteção de redes, incluindo aquisições de hardware e software e respectivo serviço de implantação, posterior monitoramento e suporte técnico 24x7x365, onde representam passos essenciais para garantir a integridade, disponibilidade e confidencialidade das informações governamentais.

5. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERANDO TODO O CICLO DE VIDA DO OBJETO

5.1. A descrição da solução como um todo encontra-se pormenorizada no **"ANEXO A ESPECIFICAÇÕES DETALHADAS"** deste Termo.

6. DA EXECUÇÃO DO OBJETO

6.1. O prazo de execução do objeto contratual será de 12 (doze) meses para os itens 1 a 28 e de 36 (trinta e seis) meses para os itens 29 a 35, contado a partir do recebimento da ordem de serviço ou instrumento equivalente.

6.1.1. O prazo de execução poderá ser prorrogado, nos termos da Lei Federal n° 14.133/2021, e para as empresas públicas e sociedades de economia mista, o disposto na Lei Federal nº 13.303/2016.

6.2. Condições de Entrega

6.2.1. Os itens 1 a 21 do objeto contratual deverão ser entregues na Contratante em conformidade com as especificações e condições estabelecidas neste termo, no prazo de 90 (noventa) dias úteis, contado do recebimento da ordem de fornecimento ou instrumento equivalente, nos locais, horários e dias estabelecidos no respectivo documento.

6.2.2. Os atrasos ocasionados por motivo de força maior ou caso fortuito, desde que justificados e aceitos pelo contratante, não serão considerados como inadimplemento contratual.

6.3. Da Garantia, manutenção, suporte e assistência

6.3.1 A CONTRATADA dará suporte e assistência técnica 24x7 conforme descrito abaixo caso um dos itens 29 a 34 seja contratado, pelo período de 36 (trinta e seis) meses.

6.3.2 O suporte e assistência técnica se dará conforme as condições especificadas a partir do item 6.3.3. deste TR caso nenhum dos itens 29 a 34 seja contratado.

6.3.2.1 A CONTRATADA deverá possuir uma solução de monitoramento conforme Anexo C.

6.3.2.2 A CONTRATANTE poderá solicitar qualquer relatório da solução com uma frequência mensal o que deverá ser provido pela contratada num prazo de 5 dias úteis.

6.3.2.3 A CONTRATADA também será responsável pela administração e manutenção do serviço em regime de 24x7x365 para atendimentos remotos e o regime 8x5 para atendimentos que possam ser necessários na forma presencial, durante todo o período do serviço contemplado nesse Edital. As tarefas atinentes ao trans porte, deslocamento e remessa necessários, seja na implementação, substituição e/ ou remoção de equipamentos defeituosos será de responsabilidade da CONTRATADA.

6.3.2.4 Para garantir a qualidade e disponibilidade do serviço, deverá ser disponibilizado pela empresa CONTRATADA uma ferramenta de monitoramento com estrutura dedicada para a Etice que atenda as características mínimas descritas no ANEXO C. Essas características deverão constar na comprovação ponto-a-ponto que será entregue.

6.3.2.5 A ferramenta deve ser acompanhada de todos os itens necessários para operacionalização, tais como: softwares de apoio (sistema operacional, etc) e licenças de softwares;

6.3.2.6 O serviço de monitoramento 24x7 deverá ser prestado OBRIGATÓRIA E INDISPENSAVELMENTE através de NOCs (Network Operation Center) redundantes da empresa CONTRATADA que já deverão estar em pleno funcionamento até a data da assinatura do Contrato. Será o ponto único de contato com a equipe técnica da CONTRATANTE para abertura de chamados, incidentes, problemas, dúvidas e requisições relacionadas aos serviços contratados, atuando como a primeira instância de atendimento à CONTRATANTE.

6.3.2.7 Os serviços prestados pelo NOC compreendem, entre outros, os seguintes procedimentos:

6.3.2.7.1 Monitoramento pró-ativo do ambiente de rede WAN do CONTRATANTE;

6.3.2.7.2 Suporte técnico para identificação e resolução de problemas em software e hardware;

6.3.2.7.3 Resolução de problemas quanto acesso à internet, sites remotos, serviços de rede oferecidos aos funcionários do CONTRATANTE;

6.3.2.7.4 Resolução de problemas referente aos meios de Acesso WAN, tais como: MPLS e Ethernet;

6.3.2.7.5 Suporte em criação de políticas, configurações, parametrizações de quaisquer ordens

relativos aos equipamentos ofertados;

6.3.2.7.6 Resolução de problemas referente a políticas, configurações, parametrizações de quaisquer ordens relativos aos equipamentos ofertados;

6.3.2.7.7 Suporte à criação, geração e parametrização de relatórios e eventos de segurança de quaisquer naturezas detectados e prevenidos pelos equipamentos ofertados;

6.3.2.7.8 Encaminhar incidentes ao fabricante da solução;

6.3.2.7.9 Suporte em demais configurações de segurança, redundância e gerência;

6.3.2.7.10 Suporte, administração e monitoramento das políticas e tarefas de backup das configurações;

6.3.2.7.11 Apoio técnico para tarefas de auditoria e análise de logs.

6.3.2.8 A CONTRATADA deverá agir de forma reativa para incidentes, restabelecimento do serviço o mais rápido possível minimizando o impacto, seja por meio da uma solução de contorno ou definitiva. Ainda caberá a CONTRATADA agir de forma proativa aplicando medidas para a boa manutenção afim de garantir a regularidade da operação do serviço.

6.3.2.9 O atendimento e suporte técnico especializado de 1° (primeiro nível) será sempre telefônico e remoto em regime 24x7 e assim, responsável pelo acompanhamento e gestão dos chamados, controle dos Indicadores de monitoramento, atuando como ponto único de contato entre a CONTRATANTE e profissionais da equipe da CONTRATADA.

6.3.2.10 O atendimento e suporte técnico especializado de 2° (segundo nível) poderá serpresencial ou remoto em regime 8x5 em todo estado do Ceará caso o suporte remoto não seja suficiente para resolução do problema. Responsável pela prevenção e resolução de incidentes, problemas e requisições, identificando a causa raiz de eventual problema e buscando sua solução. Execução de atividades remotas e/ou presenciais em incidentes, solicitações de maior complexidade.

6.3.2.11 Os Técnicos deverão ser capacitados e certificados para prestação dos serviços, resolução de incidentes, problemas e solicitações nos equipamentos ofertados. O comparecimento de um técnico ao local da necessidade será de no máximo 48 (quarenta e oito) horas para atendimentos na área que abrange e define a Região Metropolitana de Fortaleza e de até 5 (cinco) dias para as outras demais localidades (interior do Estado) e devendo sempre atender aos critérios de SLA determinados nesse Edital.

6.3.2.12 Para abertura dos chamados de suporte, a CONTRATADA deverá disponibilizar número telefônico 0800 (ou equivalente a ligação local), também serviço via portal WEB e/ou e-mail (em português). Na abertura do chamado, o órgão ao fazê-lo, receberá naquele momento, o número, data e hora de abertura do chamado. Este será considerado o início para contagem dos SLAS. O fechamento do chamado deverá ser comunicado pela CONTRATADA para fins de contagem do tempo de atendimento e resolução do chamado.

6.3.2.13 A CONTRATADA deverá possuir na sua equipe profissionais com as seguintes certificações obrigatórias e indispensáveis em face da complexidade da prestação dos serviços requeridos e ainda mais da rede computacional:

6.3.2.13.1 02 (dois) profissionais com certificação de nível técnico fornecida pelo fabricante das soluções de Next Generation Firewall ofertadas;

6.3.2.13.2 02 (dois) profissionais com certificação de nível técnico fornecida pelo fabricante das soluções de Firewall de Aplicação Web – WAF;

6.3.2.13.3 02 (dois) profissionais com certificação ITIL Foundation;

6.3.2.13.4 01 (um) profissional com certificação PMP;

6.3.2.13.5 A Comprovação de que o(s) profissional(is) indicado(s) pela contratada pertence(m) ao seu quadro permanente, se dará mediante:

6.3.2.13.5.1 Apresentação de vínculo trabalhista (registro em carteira de trabalho e previdência social CTPS e ficha de empregado) em sendo o profissional empregado da licitante ou;

6.3.2.13.5.2 Apresentação de contrato social, em sendo o profissional integrante do quadro societário da licitante ou;

6.3.2.13.5.3 Apresentação de contrato de prestação de serviço regido pela legislação civil, celebrado entre o profissional e a contratada.

6.3.2.13.5.4 A CONTRATANTE poderá, em qualquer momento durante a execução do contrato, exigir a apresentação das documentações referidas nos subitens 6.3.2.13, concedendo à

CONTRATADA o prazo improrrogável de 30 (trinta) dias corridos, contados a partir da data do requerimento, para comprovar o atendimento das exigências. Ademais, a CONTRATADA deverá, na fase de habilitação, assumir compromisso formal quanto à disponibilidade de corpo técnico especializado, devidamente capacitado para a execução dos serviços previstos no contrato, sob pena de desclassificação.

6.3.2.14 A atualização de firmware quando disponibilizado exclusivamente pelo próprio fabricante dos equipamentos deverá ser executada pela CONTRATADA sem custo adicional, sempre que requisitado pela CONTRATANTE. Toda e qualquer atualização só poderá ser aplicada mediante autorização da CONTRATANTE. As atualizações deverão ocorrer em data e horário determinado pela CONTRATADA em comum acordo e autorização da CONTRATANTE visando manter em normal funcionamento a rede onde estiverem funcionando.

6.3.2.15 A CONTRATADA deverá fornecer informações de monitoramento on-line, via dashboard que permita o acompanhamento em tempo real do estado dos ativos. Deverá ainda apresentar relatórios mensais, por meio digital (DOCX, XLSX ou PDF), com o diagnóstico e controle dos equipamentos monitorados (dados, informações, descrição, indicadores e métricas que permitam quantificar o desempenho e a disponibilidade da ope ração do serviço).

6.3.2.16 A CONTRATADA deverá disponibilizar uma ferramenta de Service Desk comprovadamente aderente as boas práticas do ITIL e que contenha o detalhamento dos chamados com no mínimo as seguintes informações: o funcionário do órgão/entidade que realizou a abertura do chamado, data e hora de abertura, data e hora de atendimento, data e hora de solução, o funcionário do órgão/entidade que realizou o encerramento do chamado, descrição detalhada do problema e das ações tomadas para sua resolução e a relação dos equipa mentos ou componentes substituídos, especificando marca, modelo, fabricante e número de série).

6.3.2.17 Os relatórios de chamados abertos poderão ser solicitados a qualquer instante pela CONTRATANTE dentro das condições estipuladas, respeitando, no entanto, um prazo de até 48 (quarenta e oito) horas uteis. Esses relatórios deverão ser retidos pelo tempo mínimo equivalente a vigência do contrato e após o seu encerramento inutilizados.

6.3.2.18 A CONTRATADA deverá comunicar ao CONTRATANTE, os casos de eminente falha operacional dos equipamentos ou de qualquer outra ação que possa vir a colocar em risco a operação da rede dela, mesmo que a falha não tenha sido consumada, mas que tenha sido detectada a existência do risco.

6.3.2.19 A CONTRATANTE deverá definir pessoas do seu Quadro de Funcionários que terão acesso de Administração nos equipamentos disponibilizados e essas pessoas deverão comunicar à empresa CONTRATADA qualquer alteração de configuração realizada nos equipamentos fornecidos nessa contratação e nessa situação respondendo por sua conta e risco pelas intervenções que possam ter efetuado.

6.3.2.20 A CONTRATADA deverá respeitar os tempos máximos de ATENDIMENTOS e SLA

(Nível de Acordo de Serviço) abaixo descritos, sob a pena de multa no caso de falhas em seu integral cumprimento:

6.3.2.20.1 Operação parada (incidente que gere parada total de algum serviço contemplado nesse contrato) o tempo de atendimento será de até 2 (duas) horas.

6.3.2.20.2 Operação impactada (incidente que gere parada parcial de algum serviço contemplado

nesse contrato) o tempo de atendimento será de até 4 (quatro) horas.

6.3.2.20.3 Requisição de serviço (solicitações de mudanças nos equipamentos ou serviços do contrato) o tempo de atendimento será de até 8 (oito) horas.

6.3.2.20.4 Informações de contrato (solicitação de informação, parecer ou relatório de algum serviço contemplado no contrato) o tempo de atendimento será de até 12 (doze) horas.

6.3.3 Os itens 1 a 21 deste TR devem oferecer as condições de garantia conforme descrito abaixo:

6.3.3.1 A garantia deverá ser integral de, no mínimo, 36 (trinta e seis) meses do fabricante, com cobertura total para peças, atualização de versão e assistência técnica.

6.3.3.2 A Assistência Técnica deverá disponibilizar número telefônico 0800 (ou equivalente ao serviço gratuito) e serviço WEB ou e-mail (em português), para registro do chamado de assistência técnica e suporte. Em relação a abertura do chamado, o órgão ao fazê-lo, receberá neste momento, o número, data e hora de abertura do chamado. Este será considerado o início para contagem dos prazos estabelecidos;

6.3.3.3 Caso seja impossível a substituição dos equipamentos, componentes, materiais ou peças por outras que não as que compõem o item proposto, esta substituição obedecerá ao critério de compatibilidade, que poderá ser encontrado no site do fabricante, através de equivalência e semelhança, e só poderá ser efetuada mediante expressa autorização por escrito do órgão/entidade, para cada caso particular. Caso o órgão/entidade recuse o equipamento, componente, material e ou peça a ser substituído, o licitante deverá apresentar alternativas, porém o prazo para solução do problema não será alterado.

7. MODELO DE GESTÃO DO CONTRATO

7.1. 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.

7.2. Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

7.3. As comunicações entre o órgão ou entidade e o contratado devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

7.4. O contratante poderá convocar representante do contratado para adoção de providências que devam ser cumpridas de imediato.

7.5. Após a assinatura do contrato ou instrumento equivalente, o contratado poderá convocar o representante do contratado para reunião inicial para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução do contratado, quando houver, do método de aferição dos resultados, quando houver, e das sanções aplicáveis, dentre outros.

7.6. A execução do contrato deverá ser acompanhada e fiscalizada pelo fiscal do contrato, ou pelo respectivo substituto, nos termos da lei.

7.7. A fiscalização se responsabilizará pelo acompanhamento da execução do objeto contratual, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração.

7.7.1. O fiscal do contrato anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados.

7.7.2. Identificada qualquer inexatidão ou irregularidade, o fiscal emitirá notificações para a correção da execução do contrato, determinando prazo para a correção.

7.7.3. O fiscal informará ao gestor do contato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso.

7.7.4 No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal comunicará o fato imediatamente ao gestor do contrato.

7.7.5. O fiscal comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual.

7.8. O gestor do contrato coordenará a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração.

7.9. O gestor do contrato acompanhará a manutenção das condições de habilitação do contratado, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais.

7.10. O gestor do contrato acompanhará os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência.

7.11. O gestor do contrato emitirá documento comprobatório da avaliação realizada pelos fiscais quanto ao cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, quando for o caso, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações.

7.12. O gestor do contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido por comissão constituída para este fim.

8. CONDIÇÕES DE RECEBIMENTO E DE PAGAMENTO

8.1. Recebimento do Objeto

8.1.1. Os bens serão recebidos **provisoriamente,** de forma sumária, no ato da entrega, juntamente com a nota fiscal ou instrumento de cobrança equivalente, pelo(a) responsável pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes neste termo e na proposta.

8.1.2. Os bens poderão ser rejeitados, no todo ou em parte, inclusive antes do recebimento provisório, quando em desacordo com as especificações constantes neste termo e na proposta, devendo ser substituídos no prazo de **90 (noventa) dias,** a contar da notificação do contratado, às suas custas, sem prejuízo da aplicação das penalidades.

8.1.3. O recebimento definitivo ocorrerá no prazo de 10(dez) dias úteis, a contar do recebimento da nota fiscal ou instrumento de cobrança equivalente pela Administração, após a verificação da qualidade e quantidade do material e consequente aceitação mediante termo detalhado.

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

8.1.5. No caso de controvérsia sobre a execução do objeto, quanto à qualidade e quantidade, deverá ser comunicando-se ao contratado para emissão de nota fiscal no que pertine à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

8.1.6. O prazo para a solução, pelo contratado, de inconsistências na execução do objeto ou de saneamento da nota fiscal ou de instrumento de cobrança equivalente, verificadas pela Administração durante a análise prévia à liquidação de despesa, não será computado para os fins do recebimento definitivo.

8.1.7. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança dos bens objeto da contratação, nem a responsabilidade ético-profissional pela perfeita execução do contrato.

8.2. Liquidação

8.2.1. Recebida a nota fiscal ou documento de cobrança equivalente, correrá o prazo de 10 (dez) dias úteis para fins de liquidação, prorrogáveis por igual período.

8.2.1.1. O prazo de que trata o subitem anterior será reduzido à metade, mantendo-se a possibilidade de prorrogação, no caso de contratações decorrentes de despesas cujos valores não ultrapassem o limite permitido para dispensa de licitação;

8.2.2. A liquidação da despesa consiste na verificação do direito adquirido pelo credor tendo por base os títulos e documentos comprobatórios do respectivo crédito, observando-se o disposto no art. 63 da Lei nº 4.320, de 17 de março de 1964.

8.2.3. Havendo erro na apresentação da nota fiscal ou documento 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;

8.2.4. A nota fiscal ou documento de cobrança equivalente deverá ser obrigatoriamente acompanhado da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no subitem 10.4 do edital.

8.2.5. A Administração deverá realizar consulta ao SICAF para: a) verificar a manutenção das condições de habilitação exigidas no edital; b) identificar possível razão que implique proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas.

8.2.6. Constatando-se, junto ao SICAF, a situação de irregularidade do contratado, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do contratante.

8.2.7. Não havendo regularização ou sendo a defesa considerada improcedente, o contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência do contratado, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

8.2.8. Persistindo a irregularidade, o contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada ao contratado a ampla defesa.

8.2.9. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso o contratado não regularize sua situação.

8.3. Prazo de pagamento

8.3.1. O pagamento será efetuado no prazo de até 30 (trinta) dias úteis, contados da finalização da liquidação da despesa.

8.3.2. No caso de atraso pelo contratante, os valores devidos ao contratado serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, mediante aplicação do índice IPCA de correção monetária.

8.4. Forma de pagamento

8.4.1. O pagamento será realizado mediante crédito em conta corrente do contratado, exclusivamente no Banco Bradesco S/A, conforme Lei nº 15.241/2012, e para as empresas pública e sociedades de economia mista, nas instituições bancárias indicadas nos respectivos Regulamentos Internos de Licitações e Contratos.

8.4.2. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

8.4.3. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

8.4.3.1. Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.

8.4.4. O contratado regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123/2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

8.5. Antecipação de Pagamento

8.5.1. É vedada a realização de pagamento antes da execução do objeto ou se o mesmo não estiver de acordo com as especificações deste instrumento.

9. DAS OBRIGAÇÕES DO CONTRATANTE

9.1. Exigir o cumprimento de todas as obrigações assumidas pelo contratado, de acordo com este instrumento e seus anexos;

9.2. Receber o objeto no prazo e condições estabelecidas neste Termo;

9.3. Notificar o contratado, por escrito, sobre vícios, defeitos ou incorreções verificadas no objeto contratado, para que seja por ele substituído, reparado ou corrigido, no total ou em parte, às suas expensas;

9.4. Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações pelo contratado;

9.5. Comunicar o contratado para emissão de nota fiscal relativa à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento, quando houver controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade;

9.6. Efetuar o pagamento ao contratado do valor correspondente a execução do objeto, no prazo, forma e condições estabelecidos neste termo;

9.7. Aplicar as sanções previstas na lei e edital, quando do descumprimento de obrigações pelo contratado;

9.8. Emitir explicitamente decisão sobre todas as solicitações e reclamações relacionadas à execução do contrato, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do contrato.

9.8.1. A Administração terá o prazo de 10 (dez) dias, a contar da data do protocolo do requerimento para decidir sobre a solicitação de prorrogação motivada.

9.9. Responder eventuais pedidos de restabelecimento do equilíbrio econômico-financeiro feitos pelo contratado no prazo máximo de 30 (trinta) dias.

9.10. Não responder por quaisquer compromissos assumidos pelo contratado com terceiros, ainda

que vinculados à execução do contrato, bem como por qualquer dano causado a terceiros em decorrência de ato do contratado, de seus empregados, prepostos ou subordinados.

10. DAS OBRIGAÇÕES DO CONTRATADO

10.1. O contratado deve cumprir todas as obrigações constantes do edital e seus anexos, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto, observando, ainda, as obrigações a seguir dispostas:

10.1.1. Entregar o objeto, quando for o caso, acompanhado do manual do usuário, com uma versão em português, e da relação da rede de assistência técnica autorizada;

10.1.2. Responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com o Código de Defesa do Consumidor;

10.1.3. Comunicar ao contratante, no prazo máximo de 24 (vinte e quatro) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação;

10.1.4. Atender às determinações regulares emitidas pelo fiscal ou gestor do contrato ou autoridade superior e prestar todo esclarecimento ou informação por eles solicitados;

10.1.5. Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os bens nos quais se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

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

10.1.7. Quando não for possível a verificação da regularidade no Sistema de Cadastramento Unificado de Fornecedores(SICAF) ou no Certificado de Registro Cadastral (CRC) do Estado do Ceará, o contratado deverá entregar ao setor responsável pela fiscalização do contrato, junto com a nota fiscal para fins de pagamento, os seguintes documentos: 1) prova de regularidade relativa à Seguridade Social; 2) Certidão Conjunta relativa aos Tributos Federais e à Dívida Ativa da União; 3) certidões que comprovem a regularidade perante a Fazenda Estadual ou Distrital do domicílio ou sede do contratado; 4) Certidão de Regularidade do FGTS – CRF; e 5) Certidão Negativa de Débitos Trabalhistas – CNDT;

10.1.8. Responsabilizar-se pelo cumprimento de todas as obrigações trabalhistas, previdenciárias, fiscais, comerciais e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade ao contratante e não poderá onerar o objeto do contrato;

10.1.9. Comunicar ao fiscal do contrato, no prazo de 24 (vinte e quatro) horas, qualquer ocorrência anormal ou acidente que se verifique no local da execução do objeto.

10.1.10. Paralisar, por determinação do contratante, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de pessoas ou bens de terceiros.

10.1.11. Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições exigidas para habilitação na licitação.

10.1.12. Cumprir, durante todo o período de execução do contrato e desde que regulamentado, a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, bem como as reservas de cargos previstas em outras normas específicas. Esta obrigação não se aplica às contratações decorrentes da Lei nº 13.303/2016.

10.1.12.1. Comprovar as reservas de cargos e vagas a que se referem o subitem acima, no prazo fixado pelo fiscal do contrato, com a indicação dos empregados que preencheram as referidas

vagas.

10.1.13. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato.

10.1.14. Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da contratação, exceto para restabelecer o equilíbrio econômico-financeiro inicial do contrato em caso de força maior, caso fortuito ou 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.

10.1.15. Não permitir a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos, nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre.

10.1.16. Promover, se for o caso, a guarda, manutenção e vigilância de materiais, ferramentas, e tudo o que for necessário à execução do objeto, durante a vigência do contrato.

10.1.17. Providenciar a substituição de qualquer profissional envolvido na execução do objeto contratual, cuja conduta seja considerada indesejável pela fiscalização do contratante.

10.1.18. Respeitar os princípios de proteção de dados pessoais elencados na Lei Geral de Proteção de Dados, Lei nº 13.709 de 14 de agosto de 2018 e suas alterações.

10.1.19. Realizar os serviços de manutenção e assistência técnica nos locais indicados pela CONTRATANTE;

10.1.19.1. O técnico deverá se deslocar ao local da execução do serviço, salvo se puder ser realizado a distância.

11. DOS ANEXOS DO TERMO DE REFERÊNCIA

ANEXO A – ESPEFICIFICAÇÕES DETALHADAS

ANEXO B - ESPECIFICAÇÕES DA SOLUÇÃO DE GERÊNCIA CENTRALIZADA E RELATORIA

ANEXO C – PLATAFORMA DE MONITORAMENTO

ANEXO D – ÓRGÃO(S) PARTICIPANTE(S)

ANEXO E – COMPROVAÇÃO DAS ESPECIFICAÇÕES TÉCNICAS

ANEXO A – ESPECIFICAÇÃO DETALHADAS

1. Especificação Detalhada dos Itens:

, nos termos da lei

Grupo único – Soluções de Firewall			
ITEM	**DESCRIÇÃO**	**UNIDADE**	**QTDE**
1	NEXT GENERATION FIREWALL – UNIDADE TIPO I	UNIDADE	1000
2	NEXT GENERATION FIREWALL – UNIDADE TIPO II	UNIDADE	50
3	NEXT GENERATION FIREWALL – UNIDADE TIPO III	UNIDADE	20
4	NEXT GENERATION FIREWALL – UNIDADE TIPO IV	UNIDADE	10
5	NEXT GENERATION FIREWALL – SEDE TIPO I	UNIDADE	8
6	NEXT GENERATION FIREWALL – SEDE TIPO II	UNIDADE	12
7	NEXT GENERATION FIREWALL – SEDE TIPO III	UNIDADE	8
8	NEXT GENERATION FIREWALL – DATA CENTER TIPO I	UNIDADE	6
9	NEXT GENERATION FIREWALL – DATA CENTER TIPO II	UNIDADE	4
10	NEXT GENERATION FIREWALL – DATA CENTER TIPO III	UNIDADE	4
11	NEXT GENERATION FIREWALL PARA AMBIENTES VIRTUALIZADOS EM NUVEM PRIVADA (1 QUANTIDADE PARA CADA CORE)	UNIDADE	30
12	SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO E RELATÓRIOS PARA ATÉ 5 EQUIPAMENTOS	SERVIÇO	8
13	SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO E RELATÓRIOS PARA ATÉ 10 EQUIPAMENTOS	SERVIÇO	6
14	SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO E RELATÓRIOS PARA ATÉ 50 EQUIPAMENTOS	SERVIÇO	4
15	SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO E RELATÓRIOS PARA ATÉ 150 EQUIPAMENTOS	SERVIÇO	4
16	SOLUÇÃO DE NEXT GENERATION ANTI-MALWARE PARA NOTEBOOKS, DESKTOPS E SERVIDORES	SERVIÇO	10000
17	SOLUÇÃO DE PREVENÇÃO DE AMEAÇAS PARA DISPOSITIVOS MÓVEIS ANDROID E IOS	SERVIÇO	2000
18	SOLUÇÃO DE PREVENÇÃO DE AMEAÇAS E SPAM PARA E-MAIL EM NUVEM – OFFICE 365 E GOOGLE	SERVIÇO	2000

	WORKSPACE		
19	FIREWALL DE APLICAÇÃO WEB – WAF - VIRTUAL	UNIDADE	10
20	FIREWALL DE APLICAÇÃO WEB – WAF – DATACENTER TIPO I	UNIDADE	8
21	FIREWALL DE APLICAÇÃO WEB – WAF – DATACENTER TIPO II	UNIDADE	4
22	INSTALAÇÃO FIREWALL UNIDADE ATÉ 100KM	SERVIÇO	500
23	INSTALAÇÃO FIREWALL UNIDADE ATÉ 400KM	SERVIÇO	300
24	INSTALAÇÃO FIREWALL UNIDADE ACIMA DE 400KM	SERVIÇO	300
25	INSTALAÇÃO FIREWALL SEDE	SERVIÇO	28
26	INSTALAÇÃO FIREWALL DATA CENTER	SERVIÇO	14
27	INSTALAÇÃO FIREWALL DE APLICAÇÃO WEB – WAF – VIRTUAL	SERVIÇO	10
28	INSTALAÇÃO FIREWALL DE APLICAÇÃO WEB – WAF – DATACENTER	SERVIÇO	12
29	SERVIÇO DE MONITORAMENTO E SUPORTE TECNICO 24X7 DE FIREWALL UNIDADE TIPO 1 E 2 36 MESES	SERVIÇO	1050
30	SERVIÇO DE MONITORAMENTO E SUPORTE TECNICO 24X7 DE FIREWALL UNIDADE TIPO 3 E 4 36 MESES	SERVIÇO	30
31	SERVIÇO DE MONITORAMENTO E SUPORTE TÉCNICO 24X7 DE FIREWALL SEDE – 36 MESES	SERVIÇO	28
32	SERVIÇO DE MONITORAMENTO E SUPORTE TÉCNICO 24X7 DE FIREWALL DATA CENTER – 36 MESES	SERVIÇO	14
33	SERVIÇO DE MONITORAMENTO E SUPORTE TÉCNICO 24X7 DE FIREWALL DE APLICAÇÃO WEB – VIRTUAL – 36 MESES	SERVIÇO	10
34	SERVIÇO DE MONITORAMENTO E SUPORTE TÉCNICO 24X7 DE FIREWALL DE APLICAÇÃO WEB – DATACENTER – 36 MESES	SERVIÇO	12
35	SERVIÇO DE SOC 24X7 COM SIEM – PACOTES DE 200 EPS – 36 MESES	SERVIÇO	30

1.1. ESPECIFICAÇÃO DETALHADA:

1.1.1. ITEM 1 NEXT GENERATION FIREWALL UNIDADE TIPO 1

1.1.1.1. CARACTERÍSTICAS GERAIS

1.1.1.1.1. É permitida a composição da solução ofertada entre diversos fabricantes, desde que não contemple solução de software livre;

1.1.1.1.2. A solução deverá ser compatível com SNMPv2 e SNMPv3;

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

1.1.1.1.4. A comunicação entre os appliances de segurança e o módulo de gerência deve ser através de meio criptografado;

1.1.1.1.5. Os appliances de segurança devem suportar operar em cluster ativo-ativo e ativo-passivo sem a necessidade de licenças adicionais;

1.1.1.1.6. Não serão aceitos modelos em listas de end-of-sale, cuja data do fim de vendas seja anterior à data da proposta.

1.1.1.1.7. Não serão aceitos modelos em lista de end-of-support, cuja data do fim do suporte seja anterior ao fim da vigência do contrato e/ou do fim do período de garantia e suporte exigido no edital.

1.1.1.2. CAPACIDADE E QUANTIDADES

1.1.1.2.1. Throughput de, no mínimo, 330 Mbps, com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação, anti-malware e prevenção de ameaças avançadas (dia zero) habilitados simultaneamente;

1.1.1.2.2. Suporte a, no mínimo, 490.000 (quatrocentas e noventa mil) conexões ou sessões simultâneas;

1.1.1.2.3. Suporte a, no mínimo, 10.300 (dez mil e trezentas) novas conexões ou sessões por segundo;

1.1.1.2.4. Throughput de, no mínimo, 950 Mbps para conexões VPN;

1.1.1.2.5. Licenciado ou permitir, pelo menos, 100 conexões ou sessões simultâneas de VPN client-tosite;

1.1.1.2.6. Possuir, pelo menos, 6 (seis) interfaces de rede 1Gbps UTP;

1.1.1.2.7. Possuir 1 (uma) interface do tipo console ou similar;

1.1.1.2.8. O Throughput e as interfaces solicitados neste item deverão ser comprovados através de datasheet público na internet. Não serão aceitas declarações de fabricantes informando números de performance e interfaces. Caso um mesmo Throughput seja apresentado mais de uma vez em diferentes métricas, será considerado o de maior valor;

1.1.1.3. FUNCIONALIDADES DE FIREWALL

1.1.1.3.1. Deve suportar autenticação para o serviço NTP.

1.1.1.3.2. Deve ser possível definir por quais origens de rede são permitidas as conexões do administrador.

1.1.1.3.3. Deve ser possível restringir o acesso à gerência do equipamento por, pelo menos, endereço IP e Rede.

1.1.1.3.4. Deve suportar SNMP v2 e v3.

1.1.1.3.5. Deve ser possível realizar captura de pacotes diretamente na gerência do equipamento.

1.1.1.3.6. Deve ser possível monitorar a utilização de CPU e memória diretamente na gerência do

equipamento.

1.1.1.3.7. Deve ser possível realizar a configuração do cluster diretamente na gerência do equipamento.

1.1.1.3.8. Deve ser possível conectar a serviços de DDNS;

1.1.1.3.9. Deve ser possível configurar o timeout da sessão do administrador na interface web.

1.1.1.3.10. Deve ser possível configurar a complexidade da senha do administrador e dias para expirar.

1.1.1.3.11. A solução deve ser capaz de trabalhar com identidades de usuários para propósitos de configurações e logs.

1.1.1.3.12. A solução deve possibilitar ao administrador realizar a integração com o AD (Active Directory) através de um assistente de configuração na própria interface gráfica do produto;

1.1.1.3.13. A solução deve identificar usuários das seguintes fontes pelo menos:

1.1.1.3.14. Active Directory: o gateway de segurança deve realizar consulta aos servidores AD para obter informação dos usuários;

1.1.1.3.15. Autenticação via navegador: para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador;

1.1.1.3.16. A identificação do usuário registrado no Microsoft Active Directory, deverá ocorrer sem qualquer tipo de agente instalado nos controladores de domínio e estações dos usuários;

1.1.1.3.17. Na integração com o AD, a operação de cadastro deve ser realizada na própria gerência do equipamento, de maneira simples e sem utilização de scripts de comando;

1.1.1.4. FUNCIONALIDADE DE PREVENÇÃO DE AMEAÇAS

1.1.1.4.1. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS integrados no próprio equipamento sem a necessidade de uso de quaisquer interfaces ou dispositivos externos.

1.1.1.4.2. Deve ser possível agendar para que o mecanismo de inspeção receba e implemente atualizações para os ataques emergentes sem a necessidade de reiniciar o equipamento;

1.1.1.4.3. Deve ser possível realizar a atualização manualmente sem necessidade de internet através da importação do pacote de atualização.

1.1.1.4.4. Deve incluir a habilidade de detectar e bloquear ataques conhecidos, protegendo, pelo menos, os seguintes ataques conhecidos: SQL Injection, ICMP Denial of Service, força bruta, scanning de portas, CIFS Port overflow, Non Compliant DNS, Non Compliant SMTP, Non Compliant CIFS, Non Compliant MS SQL Server, IKE aggressive Exchange;

1.1.1.4.5. Deve ser capaz de bloquear tráfego SSH em DNS tunneling;

1.1.1.4.6. A solução deverá ser capaz de inspecionar e proteger apenas hosts internos ou inspecionar todo o tráfego;

1.1.1.4.7. A solução deve proteger contra-ataques do tipo envenenamento de cache DNS (DNS Cache Poisoning);

1.1.1.4.8. A solução deverá possuir pelo menos dois perfis pré-configurados de fábrica para uso imediato e permitir a customização de um perfil;

1.1.1.4.9. Em cada proteção de segurança, devem estar inclusas informações como: categoria, tipo de impacto na ferramenta, severidade, e tipo de ação que a solução irá executar;

1.1.1.4.10. A solução de IPS deve possuir um modo de solução de problemas, que define o uso de perfil de detecção sem modificar as proteções individuais já criadas e customizadas;

1.1.1.4.11. Deve ser possível criar regras de exceção no IPS para que a solução não faça a inspeção de um tráfego específico por pelo menos proteção, origem, destino, serviço ou porta.

1.1.1.4.12. Deve ser possível visualizar a lista de proteções disponíveis no equipamento com os detalhes.

1.1.1.4.13. A solução deve incluir ferramenta própria ou solução de terceiros para mitigar/bloquear a comunicação entre os hosts infectados com bot e operador remoto (command & contrai).

1.1.1.4.14. A solução deve bloquear arquivos potencialmente maliciosos infectados com malware.

1.1.1.4.15. A solução de proteção contra malware e bot deve compartilhar a mesma política para facilitar o gerenciamento.

1.1.1.4.16. A solução de proteção contra malware e bot deve possuir um modo de solução de problemas, que define o uso de perfil de detecção, sem modificar as proteções individuais já criadas e customizadas;

1.1.1.4.17. As proteções devem ser ativadas baseadas em, pelo menos, critério de nível de confiança, ações da proteção e impacto de performance.

1.1.1.4.18. Deve ser possível habilitar a trilha das proteções para não logar, criar um log ou gerar um alerta;

1.1.1.4.19. Deve ser possível criar regras de exceção para que a solução não faça a inspeção de um tráfego específico por escopo, proteção e definir a ação e log para cada uma delas.

1.1.1.4.20. A solução de anti-malware deve suportar protocolos SMTP e P OP 3, FTP, HT TP

em qualquer porta;

1.1.1.4.21. Deve ser possível definir uma política de inspeção para os tipos de arquivos por:
1.1.1.4.22. Inspecionar tipos de arquivos conhecidos que contenham malware;

1.1.1.4.23. Inspecionar todos os tipos de arquivos;

1.1.1.4.24. Inspecionar tipos de arquivos de famílias específicas;

1.1.1.4.25. Deve bloquear acesso a URLs com malware;

1.1.1.4.26. Deve ser possível customizar a página exibida para o usuário quando a URL contiver um malware e o acesso for bloqueado;

1.1.1.5 FILTRO DE CONTEÚDO WEB

1.1.1.5.1. A solução deverá contar com ferramentas de visibilidade e controle de aplicações web e filtro URL integrada no próprio appliance de segurança que permita a criação de políticas de liberação ou bloqueio baseando-se em aplicações web e URL;

1.1.1.5.2. A gerência das políticas de segurança de controle de aplicação e controle de URL's deverá ser realizada na mesma interface web de gerenciamento;

1.1.1.5.3. Deve ser possível configurar com apenas um clique o bloqueio a sites e aplicações que representem um risco de segurança e estão categorizadas como spyware, phishing, botnet, spam, anonymizer ou hacking.

1.1.1.5.4. Deve ser possível configurar com apenas um clique o bloqueio a sites com conteúdo inapropriado como sexo, violência, armas, jogos e álcool.

1.1.1.5.5. Deve configurar regras para permitir ou bloquear aplicações ou páginas da Internet por pelo menos:

1.1.1.5.6. Usuário do Active Directory

1.1.1.5.7. IP

1.1.1.5.8. Rede

1.1.1.5.9. Deve ser possível configurar o bloqueio de compartilhamento de arquivos com origem usualmente ilegais como aplicações torrents e peer-to-peer.

1.1.1.5.10. Deve ser possível configurar manualmente o bloqueio de aplicações ou categorias de sites de aplicações indesejadas.

1.1.1.5.11. Deve ainda ser possível adicionar uma URL ou aplicação que não está na base de dados.

1.1.1.5.12. Deve ser possível limitar o consumo de banda de aplicações.

1.1.1.5.13. A base de aplicações deve ser superior a 2900 aplicações, reconhecendo, pelo menos, as seguintes aplicações: bittorrent, gnutella, skype, facebook, linkedin, twitter, gmail, dropbox, whatsapp, etc;

1.1.1.5.14. Deve ser possível realizar a recategorização de uma URL através da gerência do equipamento.

1.1.1.5.15. Deve ser possível customizar e definir a frequência com que serão exibidas as mensagens para os usuários nas seguintes ações:

1.1.1.5.16. Aceitar e informar

1.1.1.5.17. Bloquear e informar

1.1.1.5.18. Perguntar

1.1.1.6 IDENTIFICAÇÃO DE USUÁRIOS

1.1.1.6.1. A solução deve ser capaz de trabalhar com identidades de usuários para propósitos de configurações e logging.

1.1.1.6.2. A solução deve possibilitar ao administrador realizar a integração com o AD através de um assistente de configuração na própria interface gráfica do produto;

1.1.1.6.3. A solução deve identificar usuários das seguintes fontes:

1.1.1.6.4. Active Directory o gateway de segurança deve realizar consulta aos servidores AD para obter informação dos usuários;

1.1.1.6.5. Autenticação via navegador Para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador;

1.1.1.6.6. A identificação do usuário registrado no Microsoft Active Directory, deverá ocorrer sem qualquer tipo de agente instalado nos controladores de domínio e estações dos usuários;

1.1.1.6.7. Na integração com o AD, a operação de cadastro deve ser realizada na própria interface web de gerência, de maneira simples e sem utilização de scritps de comando;

1.1.1.7 FUNCIONALIDADES DE CONTROLE DE QUALIDADE DE SERVIÇO E SD-WAN

1.1.1.7.1. Suportar a criação de políticas de controle de serviço por:

1.1.1.7.1.1. Endereço de origem, endereço de destino, por porta e por aplicação;

1.1.1.7.2. Disponibilizar estatísticas em tempo real para as políticas de controle;

1.1.1.7.3. A solução deve permitir, por aplicação, o encaminhamento do tráfego para diferentes links de Internet, sejam eles locais ou remotos, deve suportar múltiplos links de acesso como MPLS, Internet Banda Larga, LTE e Satélite.

1.1.1.7.4. Deve possibilitar a utilização de configuração inteligente de acessos WAN IP ativos-ativos sem a necessidade de switch para agregação WAN, ou seja, distribuir o tráfego simultaneamente pelos N acessos conectados e não apenas na configuração dos acessos principal e backup.

1.1.1.7.5. Medir parâmetros de rede jitter, perda de pacotes e latência em tempo real.

1.1.1.7.6. Se houver necessidade de saída internet do ponto remoto, deve ser possível selecionar por tipo de aplicativo

1.1.1.7.7. Deve permitir a comunicação indireta entre localidades por meio de uma topologia “hub and spoke” e "full mesh"

1.1.1.7.8. Deve balancear o tráfego de aplicativos em vários links simultaneamente

1.1.1.7.9. Redistribuição do tráfego balanceado, de forma inteligente, tendo em conta o congestionamento da largura de banda, entre os links utilizados, em caso de falhas nestes links, ou de acordo com as políticas de qualidade pré-definidas

1.1.1.7.10. Habilitar a mesma interface WAN para enviar tráfego simultaneamente por meio de túneis IPSec SD-WAN e nativamente fora dos túneis via underlay.

1.1.1.7.11. Habilitar a criação de políticas de negócios para controlar o padrão de redirecionamento de tráfego e aplicar qualidade de serviço

1.1.1.7.12. Suportar políticas inteligentes usando configurações executem redirecionamento automático e imposição de QoS de voz, vídeo e tráfego transacional

1.1.1.7.13. Suportar o redirecionamento do tráfego de internet de pontos remotos para um ponto de internet centralizado, usando políticas por aplicativo

1.1.1.7.14. Redirecionamento condicionado do tráfego de internet em caso de falha do link de internet local ou do link remoto centralizado, utilizando políticas por aplicativo.

1.1.1.7.15. Suporte simultâneo ao redirecionamento do tráfego da Web de alguns aplicativos para a Internet centralizada, outros aplicativos para a Internet local e outros aplicativos para inspeção avançada de segurança na nuvem.

1.1.1.7.16. Implementar o conceito de perfis de configuração e grupos de objetos para automatizar o processo de implementação de políticas em grande escala sem limitação da quantidade de perfis em uso.

1.1.1.7.17. Deve ser capaz de criar um túnel otimizado que proteja os aplicativos TCP e UDP contra jitter e perda de pacotes para garantir desempenho de ponta a ponta para áudio, vídeo e tráfego transacional.

1.1.1.7.18. Usar probes artificiais baseadas em icmp para medir a qualidade da rede percebida pelo tráfego do usuário, medindo no minimo jitter, latencia e perda de pacotes.

1.1.1.7.19. Capacidade de realizar agregação de largura de banda automaticamente entre links de diferentes velocidades, levando em consideração o uso total da largura de banda de cada link sem causar congestionamento em links de baixa velocidade.

1.1.1.7.20. Habilitar a configuração de backup do link, ou seja, um link de backup só deve ser ativado quando o link principal falhar.

1.1.1.7.21. Implementar um mecanismo de proteção de variação de latência (jitter) mesmo que a degradação esteja em todos os links, para proteger o tráfego em tempo real (voz e vídeo).

1.1.1.7.22. Garantir o desempenho de aplicativos em um cenário de link de transporte duplo quando ambos os links estão degradados simultaneamente

1.1.1.7.23. Possuir um mecanismo de priorização para proteger o tráfego de aplicativos prioritários quando houver congestionamento em pontos remotos

1.1.1.7.24. Deve automatizar o reconhecimento dos melhores níveis de SLA de rede com base no tipo de tráfego seja áudio, vídeo ou transacional.

1.1.1.7.25. O console de gerenciamento deve informar o status operacional das interfaces LAN e WAN

1.1.1.7.26. O console de gerenciamento deve informar o status operacional de cada dispositivo que faz parte da rede para operacionalidade, inclusive informando a versão da política aplicada em cada dispositivo.

1.1.1.7.27. Realizar medições de “Latência”/”Jitter”/”Queda de pacotes” em cada um dos túneis SDWAN independentemente, na direção de transmissão ou recepção

1.1.1.7.28. O Orquestrador pode estar na Nuvem ou até mesmo ser instalado em um servidor dedicado ou virtualizado, utilizando uma máquina virtual

1.1.1.7.29. No caso do Orquestrator estar na nuvem, a administração de atualizações, gerenciamento de alta disponibilidade e hardening do plano de gerenciamento deve ser realizada pelo fabricante da solução.

1.1.1.8 FUNCIONALIDADES DE ACESSO REMOTO

1.1.1.8.1. A solução deve prover acesso seguro encriptado aos usuários remotos através da Internet;

1.1.1.8.2. A solução deve prover conectividade através de um cliente instalado no computador do usuário e através do navegador do usuário com conexão segura (HTTPS).

1.1.1.8.3. Deve suportar pelo menos os seguintes métodos de conexão:

1.1.1.8.4. Conexão através de cliente instalado no laptop ou desktop do usuário.

1.1.1.8.5. Conexão através de cliente instalado no smartphone e tablets.

1.1.1.8.6. Conexão através de navegador com SSL.

1.1.1.8.7. Conexão através de cliente nativo Windows L2TP.

1.1.1.8.8. Solução deve suportar alterar a porta padrão 443 para estabelecimento de VPN SSL.

1.1.1.8.9. A solução deve permitir conexão VPN aos seguintes usuários:

1.1.1.8.10. Usuários locais na própria base do appliance.

1.1.1.8.10. Usuários locais na própria base do appliance.

1.1.1.8.11. Grupos de usuários locais na própria base do appliance.

1.1.1.8.12. Grupos de usuários do Active Directory.

1.1.1.8.13. Grupos de usuários Radius.

1.1.1.8.14. A solução deve permitir atribuir um endereço específico para o usuário remoto.

1.1.1.9 FUNCIONALIDADE DE VPN SITE-TO-SITE

1.1.1.9.1. A solução deve prover acesso seguro criptografado entre duas localidades através da Internet;

1.1.1.9.2. A solução deve estabelecer VPN com o site remoto do próprio fabricante ou de terceiros;

1.1.1.9.3. A solução deve suportar autenticação com senha ou certificado;

1.1.1.9.4. Deve suportar, pelo menos, criptografia AES 128 e 256;

1.1.1.9.5. Deve possuir mecanismo para monitorar a saúde do túnel remoto;

1.1.2. ITEM 2 - NEXT GENERATION FIREWALLUNIDADE TIPO II

1.1.2.1. CARACTERÍSTICAS GERAIS

1.1.2.1.1. É permitida a composição da solução ofertada entre diversos fabricantes, desde que

não contemple solução de software livre;

1.1.2.1.2. A solução deverá ser compatível com SNMPv2 e SNMPv3;

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

1.1.2.1.4. A comunicação entre os appliances de segurança e o módulo de gerência deve ser através de meio criptografado;

1.1.2.1.5. Os appliances de segurança devem suportar operar em cluster ativo-ativo e ativo-passivo sem a necessidade de licenças adicionais;

1.1.2.1.6. Não serão aceitos modelos em listas de end-of-sale, cuja data do fim de vendas seja anterior à data da proposta.

1.1.2.1.7. Não serão aceitos modelos em lista de end-of-support, cuja data do fim do suporte seja anterior ao fim da vigência do contrato e/ou do fim do período de garantia e suporte exigido no edital.

1.1.2.2. CAPACIDADE E QUANTIDADES

1.1.2.2.1. Throughput de, no mínimo, 650 Mbps, com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação, anti-malware e prevenção de ameaças avançadas (dia zero) habilitados simultaneamente;

1.1.2.2.2. Suporte a, no mínimo, 490.000 (quatrocentas e noventa mil) conexões ou sessões simultâneas;

1.1.2.2.3. Suporte a, no mínimo, 20.000 (vinte mil) novas conexões ou sessões por segundo;

1.1.2.2.4. Throughput de, no mínimo, 2.2 Gbps para conexões VPN;

1.1.2.2.5. Licenciado ou permitir, pelo menos, 200 conexões ou sessões simultâneas de VPN client-tosite;

1.1.2.2.6. Possuir, pelo menos, 10 (dez) interfaces de rede 1Gbps UTP;

1.1.2.2.7. Possuir, pelo menos, 1 (uma) interface de rede 1Gbps SFP;

1.1.2.2.8. Possuir 1 (uma) interface do tipo console ou similar;

1.1.2.2.9. O Throughput e as interfaces solicitados neste item deverão ser comprovados através de datasheet público na internet. Não serão aceitas declarações de fabricantes informando números de performance e interfaces. Caso um mesmo Throughput seja apresentado mais de uma vez em diferentes métricas, será considerado o de maior valor;

1.1.2.3. FUNCIONALIDADES DE FIREWALL

1.1.2.3.1. Deve suportar autenticação para o serviço NTP.

1.1.2.3.2. Deve ser possível definir por quais origens de rede são permitidas as conexões do administrador.

1.1.2.3.3. Deve ser possível restringir o acesso à gerência do equipamento por, pelo menos, endereço IP e Rede.

1.1.2.3.4. Deve suportar SNMP v2 e v3.

1.1.2.3.5. Deve ser possível realizar captura de pacotes diretamente na gerência do equipamento.

1.1.2.3.6. Deve ser possível monitorar a utilização de CPU e memória diretamente na gerência do equipamento.

1.1.2.3.7. Deve ser possível realizar a configuração do cluster diretamente na gerência do equipamento.

1.1.2.3.8. Deve ser possível conectar a serviços de DDNS;

1.1.2.3.9. Deve ser possível configurar o timeout da sessão do administrador na interface web.

1.1.2.3.10. Deve ser possível configurar a complexidade da senha do administrador e dias para expirar.

1.1.2.3.11. A solução deve ser capaz de trabalhar com identidades de usuários para propósitos de configurações e logs.

1.1.2.3.12. A solução deve possibilitar ao administrador realizar a integração com o AD (Active Directory) através de um assistente de configuração na própria interface gráfica do produto;

1.1.2.3.13. A solução deve identificar usuários das seguintes fontes pelo menos:

1.1.2.3.14. Aclive Directory: o gateway de segurança deve realizar consulta aos servidores AD para obter informação dos usuários;

1.1.2.3.15. Autenticação via navegador: para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador;

1.1.2.3.16. A identificação do usuário registrado no Microsoft Aclive Directory, deverá ocorrer sem qualquer tipo de agente instalado nos controladores de domínio e estações dos usuários;

1.1.2.3.17. Na integração com o AD, a operação de cadastro deve ser realizada na própria gerência do equipamento, de maneira simples e sem utilização de scripts de comando;

1.1.2.4. FUNCIONALIDADE DE PREVENÇÃO DE AMEAÇAS

1.1.2.4.1. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS integrados no próprio equipamento sem a necessidade de uso de quaisquer interfaces ou dispositivos externos.

1.1.2.4.2. Deve ser possível agendar para que o mecanismo de inspeção receba e implemente atualizações para os ataques emergentes sem a necessidade de reiniciar o equipamento;

1.1.2.4.3. Deve ser possível realizar a atualização manualmente sem necessidade de internet através da importação do pacote de atualização.

1.1.2.4.4. Deve incluir a habilidade de detectar e bloquear ataques conhecidos, protegendo, pelo menos, os seguintes ataques conhecidos: SQL Injection, ICMP Denial of Service, força bruta, scanning de portas, CIFS Port overflow, Non Compliant DNS, Non Compliant SMTP, Non Compliant CIFS, Non Compliant MS SQL Server, IKE aggressive Exchange;

1.1.2.4.5. Deve ser capaz de bloquear tráfego SSH em DNS tunneling;

1.1.2.4.6. A solução deverá ser capaz de inspecionar e proteger apenas hosts internos ou inspecionar todo o tráfego;

1.1.2.4.7. A solução deve proteger contra ataques do tipo envenenamento de cache DNS (DNS Cache Poisoning);

1.1.2.4.8. A solução deverá possuir pelo menos dois perfis pré-configurados de fábrica para uso imediato e permitir a customização de um perfil;

1.1.2.4.9. Em cada proteção de segurança, devem estar inclusas informações como: categoria, tipo de impacto na ferramenta, severidade, e tipo de ação que a solução irá executar;

1.1.2.4.10. A solução de IPS deve possuir um modo de solução de problemas, que define o uso de perfil de detecção sem modificar as proteções individuais já criadas e customizadas;

1.1.2.4.11. Deve ser possível criar regras de exceção no IPS para que a solução não faça a inspeção de um tráfego específico por pelo menos proteção, origem, destino, serviço ou porta.

1.1.2.4.12. Deve ser possível visualizar a lista de proteções disponíveis no equipamento com os detalhes.

1.1.2.4.13. A solução deve incluir ferramenta própria ou solução de terceiros para mitigar/bloquear a comunicação entre os hosts infectados com bot e operador remoto (command & control).

1.1.2.4.14. A solução deve bloquear arquivos potencialmente maliciosos infectados com malware.

1.1.2.4.15. A solução de proteção contra malware e bot deve compartilhar a mesma política para facilitar o gerenciamento.

1.1.2.4.16. A solução de proteção contra malware e bot deve possuir um modo de solução de problemas, que define o uso de perfil de detecção, sem modificar as proteções individuais já criadas e customizadas;

1.1.2.4.17. As proteções devem ser ativadas baseadas em, pelo menos, critério de nível de confiança, ações da proteção e impacto de performance.

1.1.2.4.18. Deve ser possível habilitar a trilha das proteções para não logar, criar um log ou gerar um alerta;

1.1.2.4.19. Deve ser possível criar regras de exceção para que a solução não faça a inspeção de um tráfego específico por escopo, proteção e definir a ação e log para cada uma delas.

1.1.2.4.20. A solução de anti-malware deve suportar protocolos SMTP e POP3, FTP, HTTP

em qualquer porta;

1.1.2.4.21. Deve ser possível definir uma política de inspeção para os tipos de arquivos por:
1.1.2.4.22. Inspecionar tipos de arquivos conhecidos que contenham malware;

1.1.2.4.23. Inspecionar todos os tipos de arquivos;

1.1.2.4.24. Inspecionar tipos de arquivos de famílias específicas;

1.1.2.4.25. Deve bloquear acesso a URLs com malware;

1.1.2.4.26. Deve ser possível customizar a página exibida para o usuário quando a URL contiver um malware e o acesso for bloqueado;

1.1.2.5. FILTRO DE CONTEÚDO WEB

1.1.2.5.1. A solução deverá contar com ferramentas de visibilidade e controle de aplicações web e filtro URL integrada no próprio appliance de segurança que permita a criação de políticas de liberação ou bloqueio baseando-se em aplicações web e URL;

1.1.2.5.2. A gerência das políticas de segurança de controle de aplicação e controle de URL's deverá ser realizada na mesma interface web de gerenciamento;

1.1.2.5.3. Deve ser possível configurar com apenas um clique o bloqueio a sites e aplicações que representem um risco de segurança e estão categorizadas como spyware, phishing, botnet, spam, anonymizer ou hacking.

1.1.2.5.4. Deve ser possível configurar com apenas um clique o bloqueio a sites com conteúdo inapropriado como sexo, violência, armas, jogos e álcool.

1.1.2.5.5. Deve configurar regras para permitir ou bloquear aplicações ou páginas da Internet por pelo menos:

1.1.2.5.5.1. Usuário do Active Directory

1.1.2.5.5.2. IP

1.1.2.5.5.3. Rede

1.1.2.5.6. Deve ser possível configurar o bloqueio de compartilhamento de arquivos com origem usualmente ilegais como aplicações torrents e peer-to-peer.

1.1.2.5.7. Deve ser possível configurar manualmente o bloqueio de aplicações ou categorias de sites de aplicações indesejadas.

1.1.2.5.8. Deve ainda ser possível adicionar uma URL ou aplicação que não está na base de dados.

1.1.2.5.9. Deve ser possível limitar o consumo de banda de aplicações.

1.1.2.5.10. A base de aplicações deve ser superior a 2900 aplicações, reconhecendo, pelo menos, as seguintes aplicações: bittorrent, gnutella, skype, facebook, linkedin, twitter, gmail, dropbox, whatsapp, etc;

1.1.2.5.11. Deve ser possível realizar a recategorização de uma URL através da gerência do equipamento.

1.1.2.5.12. Deve ser possível customizar e definir a frequência com que serão exibidas as mensagens para os usuários nas seguintes ações:

1.1.2.5.12.1. Aceitar e informar

1.1.2.5.12.2. Bloquear e informar

1.1.2.5.12.3. Perguntar

1.1.2.6. IDENTIFICAÇÃO DE USUÁRIOS

1.1.2.6.1. A solução deve ser capaz de trabalhar com identidades de usuários para propósitos de configurações e logging.

1.1.2.6.2. A solução deve possibilitar ao administrador realizar a integração com o AD através de um assistente de configuração na própria interface gráfica do produto;

1.1.2.6.3. A solução deve identificar usuários das seguintes fontes:

1.1.2.6.4. Aclive Directory o gateway de segurança deve realizar consulta aos servidores AD para obter informação dos usuários;

1.1.2.6.5. Autenticação via navegador para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador;

1.1.2.6.6. A identificação do usuário registrado no Microsoft Aclive Directory, deverá ocorrer sem qualquer tipo de agente instalado nos controladores de domínio e estações dos usuários;

1.1.2.6.7. Na integração com o AD, a operação de cadastro deve ser realizada na própria interface web de gerência, de maneira simples e sem utilização de scritps de comando;

1.1.2.7. FUNCIONALIDADES DE CONTROLE DE QUALIDADE DE SERVIÇO E SD-WAN

1.1.2.7.1. Suportar a criação de políticas de controle de serviço por:

1.1.2.7.2. Endereço de origem, endereço de destino, por porta e por aplicação;

1.1.2.7.3. Disponibilizar estatísticas em tempo real para as políticas de controle;

1.1.2.7.4. A solução deve permitir, por aplicação, o encaminhamento do tráfego para diferentes links de Internet, sejam eles locais ou remotos, deve suportar múltiplos links de acesso como MPLS, Internet Banda Larga, LTE e Satélite.

1.1.2.7.5. Deve possibilitar a utilização de configuração inteligente de acessos WAN IP ativos-ativos sem a necessidade de switch para agregação WAN, ou seja, distribuir o tráfego simultaneamente pelos N acessos conectados e não apenas na configuração dos acessos principal e backup.

1.1.2.7.6. Medir parâmetros de rede jitter, perda de pacotes e latência em tempo real.

1.1.2.7.7. Se houver necessidade de saída internet do ponto remoto, deve ser possível selecionar por tipo de aplicativo

1.1.2.7.8. Deve permitir a comunicação indireta entre localidades por meio de uma topologia “hub and spoke” e "full mesh"

1.1.2.7.9. Deve balancear o tráfego de aplicativos em vários links simultaneamente

1.1.2.7.10. Redistribuição do tráfego balanceado, de forma inteligente, tendo em conta o

congestionamento da largura de banda, entre os links utilizados, em caso de falhas nestes

links, ou de acordo com as políticas de qualidade pré-definidas

1.1.2.7.11. Habilitar a mesma interface WAN para enviar tráfego simultaneamente por meio de túneis IPSec SD-WAN e nativamente fora dos túneis via underlay.

1.1.2.7.12. Habilitar a criação de políticas de negócios para controlar o padrão de redirecionamento de tráfego e aplicar qualidade de serviço

1.1.2.7.13. Suportar políticas inteligentes usando configurações executem redirecionamento automático e imposição de QoS de voz, vídeo e tráfego transacional

1.1.2.7.14. Suportar o redirecionamento do tráfego de internet de pontos remotos para um ponto de internet centralizado, usando políticas por aplicativo

1.1.2.7.15. Redirecionamento condicionado do tráfego de internet em caso de falha do link de internet local ou do link remoto centralizado, utilizando políticas por aplicativo.

1.1.2.7.16. Suporte simultâneo ao redirecionamento do tráfego da Web de alguns aplicativos para a Internet centralizada, outros aplicativos para a Internet local e outros aplicativos para inspeção avançada de segurança na nuvem.

1.1.2.7.17. Implementar o conceito de perfis de configuração e grupos de objetos para automatizar o processo de implementação de políticas em grande escala sem limitação da quantidade de perfis em uso.

1.1.2.7.18. Deve ser capaz de criar um túnel otimizado que proteja os aplicativos TCP e UDP contra jitter e perda de pacotes para garantir desempenho de ponta a ponta para áudio, vídeo e tráfego transacional.

1.1.2.7.19. Usar probes artificiais baseadas em icmp para medir a qualidade da rede percebida pelo tráfego do usuário, medindo no minimo jitter, latência e perda de pacotes.

1.1.2.7.20. Capacidade de realizar agregação de largura de banda automaticamente entre

links de diferentes velocidades, levando em consideração o uso total da largura de banda

de cada link sem causar congestionamento em links de baixa velocidade.

1.1.2.7.21. Habilitar a configuração de backup do link, ou seja, um link de backup só deve ser ativado quando o link principal falhar.

1.1.2.7.22. Implementar um mecanismo de proteção de variação de latência (jitter) mesmo que a degradação esteja em todos os links, para proteger o tráfego em tempo real (voz e vídeo).

1.1.2.7.23. Garantir o desempenho de aplicativos em um cenário de link de transporte duplo quando ambos os links estão degradados simultaneamente

1.1.2.7.24. Possuir um mecanismo de priorização para proteger o tráfego de aplicativos prioritários quando houver congestionamento em pontos remotos

1.1.2.7.25. Deve automatizar o reconhecimento dos melhores níveis de SLA de rede com base no tipo de tráfego seja áudio, vídeo ou transacional.

1.1.2.7.26. O console de gerenciamento deve informar o status operacional das interfaces LAN e WAN

1.1.2.7.27. O console de gerenciamento deve informar o status operacional de cada dispositivo que faz parte da rede para operacionalidade, inclusive informando a versão da política aplicada em cada dispositivo.

1.1.2.7.28. Realizar medições de “Latência”/”Jitter”/”Queda de pacotes” em cada um dos túneis SDWAN independentemente, na direção de transmissão ou recepção

1.1.2.7.29. O Orquestrador pode estar na Nuvem ou até mesmo ser instalado em um servidor dedicado ou virtualizado, utilizando uma máquina virtual

1.1.2.7.30. No caso do Orquestrator estar na nuvem, a administração de atualizações, gerenciamento de alta disponibilidade e hardening do plano de gerenciamento deve ser realizada pelo fabricante da solução.

1.1.2.8. FUNCIONALIDADES DE ACESSO REMOTO

1.1.2.8.1. A solução deve prover acesso seguro encriptado aos usuários remotos através da Internet;

1.1.2.8.2. A solução deve prover conectividade através de um cliente instalado no computador do usuário e através do navegador do usuário com conexão segura (HTTPS).

1.1.2.8.3. Deve suportar pelo menos os seguintes métodos de conexão:

1.1.2.8.3.1 Conexão através de cliente instalado no laptop ou desktop do usuário.

1.1.2.8.3.2 Conexão através de cliente instalado no smartphone e tablets.

1.1.2.8.3.3 Conexão através de navegador com SSL.

1.1.2.8.3.4 Conexão através de cliente nativo Windows L2TP.

1.1.2.8.4. Solução deve suportar alterar a porta padrão 443 para estabelecimento de VPN SSL.

1.1.2.8.5. A solução deve permitir conexão VPN aos seguintes usuários:

1.1.2.8.3.5 Usuários locais na própria base do appliance.

1.1.2.8.3.6 Grupos de usuários locais na própria base do appliance.

1.1.2.8.3.7 Grupos de usuários do Aclive Directory.

1.1.2.8.3.8 Grupos de usuários Radius.

1.1.2.8.3.9 A solução deve permitir atribuir um endereço específico para o usuário remoto.

1.1.2.9. FUNCIONALIDADE DE VPN SITE-TO-SITE

1.1.2.9.1.1. A solução deve prover acesso seguro criptografado entre duas localidades através da Internet;

1.1.2.9.1.2. A solução deve estabelecer VPN com o site remoto do próprio fabricante ou de terceiros;

1.1.2.9.1.3. A solução deve suportar autenticação com senha ou certificado;

1.1.2.9.1.4. Deve suportar, pelo menos, criptografia AES 128 e 256;

1.1.2.9.1.5. Deve possuir mecanismo para monitorar a saúde do túnel remoto;

1.1.3. ITEM 3 - NEXT GENERATION FIREWALL UNIDADE TIPO III

1.1.3.1. CARACTERÍSTICAS GERAIS

1.1.3.1.1. É permitida a composição da solução ofertada entre diversos fabricantes, desde que não contemple solução de software livre;

1.1.3.1.2. A solução deverá ser compatível com SNMPv2 e SNMPv3;

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

1.1.3.1.4. A comunicação entre os appliances de segurança e o módulo de gerência deve ser através de meio criptografado;

1.1.3.1.5. Os appliances de segurança devem suportar operar em cluster ativo-ativo e ativo-passivo sem a necessidade de licenças adicionais;

1.1.3.1.6. Não serão aceitos modelos em listas de end-of-sale, cuja data do fim de vendas seja anterior à data da proposta.

1.1.3.1.7. Não serão aceitos modelos em lista de end-of-support, cuja data do fim do suporte seja anterior ao fim da vigência do contrato e/ou do fim do período de garantia e suporte exigido no edital.

1.1.3.2. CAPACIDADE E QUANTIDADES

1.1.3.2.1. Throughput de, no mínimo, 1.45 Gbps, com as funcionalidades de firewall, prevenção de intrusão,

1.1.3.2.2. controle de aplicação, anti-malware e prevenção de ameaças avançadas (dia zero) habilitados simultaneamente;

1.1.3.2.3. Suporte a, no mínimo, 2.3 (dois ponto três) milhões de conexões ou sessões simultâneas;

1.1.3.2.4. Suporte a, no mínimo, 50.000 (cinquenta mil) novas conexões ou sessões por segundo;

1.1.3.2.5. Throughput de, no mínimo, 3 Gbps para conexões VPN;

1.1.3.2.6. Licenciado ou permitir, pelo menos, 450 conexões ou sessões simultâneas de VPN client-to-site;

1.1.3.2.7. Possuir, pelo menos, 16 (dezesseis) interfaces de rede 1 Gbps UTP;

1.1.3.2.8. Possuir, pelo menos, 2 (duas) interfaces de rede 1Gbps SFP;

1.1.3.2.9. Possuir 1 (uma) interface do tipo console ou similar;

1.1.3.2.10. O Throughput e as interfaces solicitados neste item deverão ser comprovados através de datasheet público na internet. Não serão aceitas declarações de fabricantes informando números de performance e interfaces. Caso um mesmo Throughput seja apresentado mais de uma vez em diferentes métricas, será considerado o de maior valor;

1.1.3.3. FUNCIONALIDADES DE FIREWALL

1.1.3.3.1. Deve suportar autenticação para o serviço NTP.

1.1.3.3.2. Deve ser possível definir por quais origens de rede são permitidas as conexões do administrador. Deve ser possível restringir o acesso à gerência do equipamento por, pelo menos, endereço IP e

1.1.3.3.3. Deve suportar SNMP v2 e v3.

1.1.3.3.4. Deve ser possível realizar captura de pacotes diretamente na gerência do equipamento.

1.1.3.3.5. Deve ser possível monitorar a utilização de CPU e memória diretamente na gerência do equipamento.

1.1.3.3.6. Deve ser possível realizar a configuração do cluster diretamente na gerência do equipamento. Deve ser possível conectar a serviços de DONS;

1.1.3.3.7. Deve ser possível configurar o timeout da sessão do administrador na interface web.

1.1.3.3.8. Deve ser possível configurar a complexidade da senha do administrador e dias para expirar.

1.1.3.3.9. A solução deve ser capaz de trabalhar com identidades de usuários para propósitos de configurações e logs.

1.1.3.3.10. A solução deve possibilitar ao administrador realizar a integração com o AD (Active Directory) através de um assistente de configuração na própria interface gráfica do produto;

1.1.3.3.11. A solução deve identificar usuários das seguintes fontes pelo menos:

1.1.3.3.12. Active Directory: o gateway de segurança deve realizar consulta aos servidores AD para obter informação dos usuários;

1.1.3.3.13. Autenticação via navegador: para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador;

1.1.3.3.14. A identificação do usuário registrado no Microsoft Active Directory, deverá ocorrer sem qualquer tipo de agente instalado nos controladores de domínio e estações dos usuários;

1.1.3.3.15. Na integração com o AD, a operação de cadastro deve ser realizada na própria gerência do equipamento, de maneira simples e sem utilização de scripts de comando;

1.1.3.4. FUNCIONALIDADE DE PREVENÇÃO DE AMEAÇAS

1.1.3.4.1. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS integrados no próprio equipamento sem a necessidade de uso de quaisquer interfaces ou dispositivos externos.

1.1.3.4.2. Deve ser possível agendar para que o mecanismo de inspeção receba e implemente atualizações para os ataques emergentes sem a necessidade de reiniciar o equipamento;

1.1.3.4.3. Deve ser possível realizar a atualização manualmente sem necessidade de internet através da importação do pacote de atualização.

1.1.3.4.4. Deve incluir a habilidade de detectar e bloquear ataques conhecidos, protegendo, pelo menos, os seguintes ataques conhecidos: SQL Injection, ICMP Denial of Service, força bruta, scanning de portas, CIFS Port overflow, Non Compliant DNS, Non Compliant SMTP, Non Compliant CIFS, Non Compliant MS-SQL Server, IKE aggressive Exchange;

1.1.3.4.5. Deve ser capaz de bloquear tráfego SSH em DNS tunneling;

1.1.3.4.6. A solução deverá ser capaz de inspecionar e proteger apenas hosts internos ou inspecionar todo o tráfego;

1.1.3.4.7. A solução deve proteger contra-ataques do tipo envenenamento de cache DNS (DNS Cache Poisoning);

1.1.3.4.8. A solução deverá possuir pelo menos dois perfis pré-configurados de fábrica para uso imediato e permitir a customização de um perfil;

1.1.3.4.9. Em cada proteção de segurança, devem estar inclusas informações como: categoria, tipo de impacto na ferramenta, severidade, e tipo de ação que a solução irá executar;

1.1.3.4.10. A solução de IPS deve possuir um modo de solução de problemas, que define o uso de perfil de detecção sem modificar as proteções individuais já criadas e customizadas;

1.1.3.4.11. Deve ser possível criar regras de exceção no IPS para que a solução não faça a inspeção de um tráfego específico por pelo menos proteção, origem, destino, serviço ou porta.

1.1.3.4.12. Deve ser possível visualizar a lista de proteções disponíveis no equipamento com os detalhes.

1.1.3.4.13. A solução deve incluir ferramenta própria ou solução de terceiros para mitigar/bloquear a comunicação entre os hosts infectados com bot e operador remoto (command & contrai).

1.1.3.4.14. A solução deve bloquear arquivos potencialmente maliciosos infectados com malware.

1.1.3.4.15. A solução de proteção contra malware e bot deve compartilhar a mesma política para facilitar o gerenciamento.

1.1.3.4.16. A solução de proteção contra malware e bot deve possuir um modo de solução de

problemas, que define o uso de perfil de detecção, sem modificar as proteções individuais já criadas e customizadas;

1.1.3.4.17. As proteções devem ser ativadas baseadas em, pelo menos, critério de nível de confiança, ações da proteção e impacto de performance.

1.1.3.4.18. Deve ser possível habilitar a trilha das proteções para não logar, criar um log ou gerar um alerta;

1.1.3.4.19. Deve ser possível criar regras de exceção para que a solução não faça a inspeção de um tráfego específico por escopo, proteção e definir a ação e log para cada uma delas.

1.1.3.4.20. A solução de anti-malware deve suportar protocolos SMTP e POP3, FTP, HTTP em qualquer porta;

1.1.3.4.21. Deve ser possível definir uma política de inspeção para os tipos de arquivos por:
1.1.3.4.22. Inspecionar tipos de arquivos conhecidos que contenham malware;

1.1.3.4.23. Inspecionar todos os tipos de arquivos;

1.1.3.4.24. Inspecionar tipos de arquivos de famílias específicas;

1.1.3.4.25. Deve bloquear acesso a URLs com malware;

1.1.3.4.26. Deve ser possível customizar a página exibida para o usuário quando a URL contiver um malware e o acesso for bloqueado;

1.1.3.5. PREVENÇÃO DE AMEAÇAS AVANÇADAS

1.1.3.5.1. A solução deve incluir ferramenta própria ou solução de terceiros para proteção de redes contra ameaças desconhecidas em arquivos que são baixados da Internet ou anexados a e-mails.

1.1.3.5.2. A solução deve compartilhar a mesma política da proteção contra vírus e bot para facilitar o gerenciamento.

1.1.3.5.3. A solução deve trabalhar em modo de prevenção e não apenas detecção.

1.1.3.5.4. Deve permitir criar uma lista de exceção de e-mails que não devem ter seus anexos inspecionados.

1.1.3.5.5. Deve permitir criar uma lista de exceção para arquivos que não devem ser inspecionados.

1.1.3.5.6. A solução deve suportar protocolos SMTP, HTTP em qualquer porta;

1.1.3.5.7. Deve permitir configurar por tipo de arquivo as ações de inspeção ou bypass.

1.1.3.5.8. A solução deve possuir nuvem de inteligência proprietária do fabricante onde seja responsável em atualizar toda a base de segurança dos appliance através de assinaturas

1.1.3.5.9. Implementar detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF com tamanho até 15 Mb.

1.1.3.5.10. Deve permitir configurar como uma emulação em conexão http será tratada, sendo permitida até que a emulação seja concluída ou bloqueada até a emulação ser completa.

1.1.3.6. FILTRO DE CONTEÚDO WEB

1.1.3.6.1. A solução deverá contar com ferramentas de visibilidade e controle de aplicações web e filtro URL integrada no próprio appliance de segurança que permita a criação de políticas de liberação ou bloqueio baseando-se em aplicações web e URL;

1.1.3.6.2. A gerência das políticas de segurança de controle de aplicação e controle de URL's deverá ser realizada na mesma interface web de gerenciamento;

1.1.3.6.3. Deve ser possível configurar com apenas um clique o bloqueio a sites e aplicações que representem um risco de segurança e estão categorizadas como spyware, phishing, botnet, spam, anonymizer ou hacking.

1.1.3.6.4. Deve ser possível configurar com apenas um clique o bloqueio a sites com conteúdo inapropriado como sexo, violência, armas, jogos e álcool.

1.1.3.6.5. Deve configurar regras para permitir ou bloquear aplicações ou páginas da Internet por pelo menos:

1.1.3.6.5.1. Usuário do Active Directory

1.1.3.6.5.2. IP

1.1.3.6.5.3. Rede

1.1.3.6.6. Deve ser possível configurar o bloqueio de compartilhamento de arquivos com origem usualmente ilegais como aplicações torrents e peer-to-peer.

1.1.3.6.7. Deve ser possível configurar manualmente o bloqueio de aplicações ou categorias de sites de aplicações indesejadas.

1.1.3.6.8. Deve ainda ser possível adicionar uma URL ou aplicação que não está na base de dados.

1.1.3.6.9. Deve ser possível limitar o consumo de banda de aplicações.

1.1.3.6.10. A base de aplicações deve ser superior a 2900 aplicações, reconhecendo, pelo menos, as seguintes aplicações: bittorrent, gnutella, skype, facebook, linkedin, twitter, gmail, dropbox, whatsapp, etc;

1.1.3.6.11. Deve ser possível realizar a recategorização de uma URL através da gerência do equipamento.

1.1.3.6.12. Deve ser possível customizar e definir a frequência com que serão exibidas as mensagens para os usuários nas seguintes ações:

1.1.3.6.12.1. Aceitar e informar

1.1.3.6.12.2. Bloquear e informar

1.1.3.6.12.3. Perguntar

1.1.3.7. IDENTIFICAÇÃO DE USUÁRIOS

1.1.3.7.1. A solução deve ser capaz de trabalhar com identidades de usuários para propósitos de configurações e logging.

1.1.3.7.2. A solução deve possibilitar ao administrador realizar a integração com o AD através de um assis tente de configuração na própria interface gráfica do produto;

1.1.3.7.3. A solução deve identificar usuários das seguintes fontes:

1.1.3.7.3.1. Aclive Directory o gateway de segurança deve realizar consulta aos servidores AD para obter in formação dos usuários;

1.1.3.7.3.2. Autenticação via navegador para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador;

1.1.3.7.3.3. A identificação do usuário registrado no Microsoft Aclive Directory, deverá ocorrer sem qualquer tipo de agente instalado nos controladores de domínio e estações dos usuários;

1.1.3.7.3.4. Na integração com o AD, a operação de cadastro deve ser realizada na própria interface web de gerência, de maneira simples e sem utilização de scritps de comando;

1.1.3.8. FUNCIONALIDADES DE CONTROLE DE QUALIDADE DE SERVIÇO E SD-WAN

1.1.3.8.1. Suportar a criação de políticas de controle de serviço por:

1.1.3.8.2. Endereço de origem, endereço de destino, por porta e por aplicação;

1.1.3.8.3. Disponibilizar estatísticas em tempo real para as políticas de controle;

1.1.3.8.4. A solução deve permitir, por aplicação, o encaminhamento do tráfego para diferentes links de Internet, sejam eles locais ou remotos, deve suportar múltiplos links de acesso como MPLS, Internet Banda Larga, LTE e Satélite.

1.1.3.8.5. Deve possibilitar a utilização de configuração inteligente de acessos WAN IP ativos-ativos sem a necessidade de switch para agregação WAN, ou seja, distribuir o tráfego simultaneamente pelos N acessos conectados e não apenas na configuração dos acessos principal e backup.

1.1.3.8.6. Medir parâmetros de rede jitter, perda de pacotes e latência em tempo real.

1.1.3.8.7. Se houver necessidade de saída internet do ponto remoto, deve ser possível selecionar por tipo de aplicativo

1.1.3.8.8. Deve permitir a comunicação indireta entre localidades por meio de uma topologia “hub and spoke” e "full mesh"

1.1.3.8.9. Deve balancear o tráfego de aplicativos em vários links simultaneamente

1.1.3.8.10. Redistribuição do tráfego balanceado, de forma inteligente, tendo em conta o

congestionamento da largura de banda, entre os links utilizados, em caso de falhas nestes

links, ou de acordo com as políticas de qualidade pré-definidas

1.1.3.8.11. Habilitar a mesma interface WAN para enviar tráfego simultaneamente por meio de túneis IPSec SD-WAN e nativamente fora dos túneis via underlay.

1.1.3.8.12. Habilitar a criação de políticas de negócios para controlar o padrão de redirecionamento de tráfego e aplicar qualidade de serviço

1.1.3.8.13. Suportar políticas inteligentes usando configurações executem redirecionamento automático e imposição de QoS de voz, vídeo e tráfego transacional

1.1.3.8.14. Suportar o redirecionamento do tráfego de internet de pontos remotos para um ponto de internet centralizado, usando políticas por aplicativo

1.1.3.8.15. Redirecionamento condicionado do tráfego de internet em caso de falha do link de internet local ou do link remoto centralizado, utilizando políticas por aplicativo.

1.1.3.8.16. Suporte simultâneo ao redirecionamento do tráfego da Web de alguns aplicativos para a Internet centralizada, outros aplicativos para a Internet local e outros aplicativos para inspeção avançada de segurança na nuvem.

1.1.3.8.17. Implementar o conceito de perfis de configuração e grupos de objetos para automatizar o processo de implementação de políticas em grande escala sem limitação da quantidade de perfis em uso.

1.1.3.8.18. Deve ser capaz de criar um túnel otimizado que proteja os aplicativos TCP e UDP contra jitter e perda de pacotes para garantir desempenho de ponta a ponta para áudio, vídeo e tráfego transacional.

1.1.3.8.19. Usar probes artificiais baseadas em icmp para medir a qualidade da rede percebida pelo tráfego do usuário, medindo no minimo jitter, latencia e perda de pacotes.

1.1.3.8.20. Capacidade de realizar agregação de largura de banda automaticamente entre links de diferentes velocidades, levando em consideração o uso total da largura de banda de cada link sem causar congestionamento em links de baixa velocidade.

1.1.3.8.21. Habilitar a configuração de backup do link, ou seja, um link de backup só deve ser

ativado quando o link principal falhar.

1.1.3.8.22. Implementar um mecanismo de proteção de variação de latência (jitter) mesmo que a degradação esteja em todos os links, para proteger o tráfego em tempo real (voz e vídeo).

1.1.3.8.23. Garantir o desempenho de aplicativos em um cenário de link de transporte duplo quando ambos os links estão degradados simultaneamente

1.1.3.8.24. Possuir um mecanismo de priorização para proteger o tráfego de aplicativos prioritários quando houver congestionamento em pontos remotos

1.1.3.8.25. Deve automatizar o reconhecimento dos melhores níveis de SLA de rede com base no tipo de tráfego seja áudio, vídeo ou transacional.

1.1.3.8.26. O console de gerenciamento deve informar o status operacional das interfaces LAN e WAN

1.1.3.8.27. O console de gerenciamento deve informar o status operacional de cada dispositivo que faz parte da rede para operacionalidade, inclusive informando a versão da política aplicada em cada dispositivo.

1.1.3.8.28. Realizar medições de “Latência”/”Jitter”/”Queda de pacotes” em cada um dos túneis SDWAN independentemente, na direção de transmissão ou recepção

1.1.3.8.29. O Orquestrador pode estar na Nuvem ou até mesmo ser instalado em um servidor dedicado ou virtualizado, utilizando uma máquina virtual

1.1.3.8.30. No caso do Orquestrator estar na nuvem, a administração de atualizações, gerenciamento de alta disponibilidade e hardening do plano de gerenciamento deve ser realizada pelo fabricante da solução.

1.1.3.9. FUNCIONALIDADES DE ACESSO REMOTO

1.1.3.9.1. A solução deve prover acesso seguro encriptado aos usuários remotos através da Internet;

1.1.3.9.2. A solução deve prover conectividade através de um cliente instalado no computador do usuário e através do navegador do usuário com conexão segura (HTTPS).

1.1.3.9.3. Deve suportar pelo menos os seguintes métodos de conexão:

1.1.3.9.3.1. Conexão através de cliente instalado no laptop ou desktop do usuário.

1.1.3.9.3.2. Conexão através de cliente instalado no smartphone e tablets.

1.1.3.9.3.3. Conexão através de navegador com SSL.

1.1.3.9.3.4. Conexão através de cliente nativo Windows L2TP.

1.1.3.9.4. Solução deve suportar alterar a porta padrão 443 para estabelecimento de VPN SSL.

1.1.3.9.5. A solução deve permitir conexão VPN aos seguintes usuários:

1.1.3.9.5.1. Usuários locais na própria base do appliance.

1.1.3.9.5.2. Grupos de usuários locais na própria base do appliance.

1.1.3.9.5.3. Grupos de usuários do Aclive Directory.

1.1.3.9.5.4. Grupos de usuários Radius.

1.1.3.9.6. A solução deve permitir atribuir um endereço específico para o usuário remoto.

1.1.3.10. FUNCIONALIDADE DE VPN SITE-TO-SITE

1.1.3.10.1. A solução deve prover acesso seguro criptografado entre duas localidades através da

Internet;

1.1.3.10.2. A solução deve estabelecer VPN com o site remoto do próprio fabricante ou de terceiros;

1.1.3.10.3. A solução deve suportar autenticação com senha ou certificado;

1.1.3.10.4. Deve suportar, pelo menos, criptografia AES 128 e 256;

1.1.3.10.5. Deve possuir mecanismo para monitorar a saúde do túnel remoto;

1.1.4. ITEM 4 - NEXT GENERATION FIREWALL UNIDADE TIPO IV

1.1.4.1. CARACTERÍSTICAS GERAIS

1.1.4.1.1. É permitida a composição da solução ofertada entre diversos fabricantes, desde que não contemple solução de software livre;

1.1.4.1.2. A solução deverá ser compatível com SNMPv2 e SNMPv3;

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

1.1.4.1.4. A comunicação entre os appliances de segurança e o módulo de gerência deve ser através de meio criptografado;

1.1.4.1.5. Os appliances de segurança devem suportar operar em cluster ativo-ativo e ativo-passivo sem a necessidade de licenças adicionais;

1.1.4.1.6. Não serão aceitos modelos em listas de end-of-sale, cuja data do fim de vendas seja anterior à data da proposta.

1.1.4.1.7. Não serão aceitos modelos em lista de end-of-support, cuja data do fim do suporte seja anterior ao fim da vigência do contrato e/ou do fim do período de garantia e suporte exigido no edital.

1.1.4.2. CAPACIDADE E QUANTIDADES

1.1.4.2.1. Throughput de, no mínimo, 1.9 Gbps, com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação, anti-malware e prevenção de ameaças avançadas (dia zero) habilitados simultaneamente;

1.1.4.2.2. Suporte a, no mínimo, 2.3 (dois ponto três) milhões de conexões ou sessões simultâneas;

1.1.4.2.3. Suporte a, no mínimo, 65.000 (sessenta e cinco mil) novas conexões ou sessões por segundo;

1.1.4.2.4. Throughput de, no mínimo, 3.8 Gbps para conexões VPN;

1.1.4.2.5. Licenciado ou permitir, pelo menos, 450 conexões ou sessões simultâneas de VPN client-to-site;

1.1.4.2.6. Possuir, pelo menos, 16 (dezesseis) interfaces de rede 1 Gbps UTP;

1.1.4.2.7. Possuir, pelo menos, 1 (uma) interfaces de rede 1Gbps SFP;

1.1.4.2.8. Possuir, pelo menos, 1 (uma) interface de rede 10Gbps SFP+;

1.1.4.2.9. Possuir armazenamento interno de, pelo menos, 250 GB SSD;

1.1.4.2.10. Possuir 1 (uma) interface do tipo console ou similar;

1.1.4.2.10. O Throughput e as interfaces solicitados neste item deverão ser comprovados através de datasheet público na internet. Não serão aceitas declarações de fabricantes informando números de performance e interfaces. Caso um mesmo Throughput seja apresentado mais de

uma vez em diferentes métricas, será considera do o de maior valor;

1.1.4.3. FUNCIONALIDADES DE FIREWALL

1.1.4.3.1. Deve suportar autenticação para o serviço NTP.

1.1.4.3.2. Deve ser possível definir por quais origens de rede são permitidas as conexões do administrador.

1.1.4.3.3. Deve ser possível restringir o acesso à gerência do equipamento por, pelo menos, endereço IP e Rede;

1.1.4.3.4. Deve suportar SNMP v2 e v3.

1.1.4.3.5. Deve ser possível realizar captura de pacotes diretamente na gerência do equipamento.

1.1.4.3.6. Deve ser possível monitorar a utilização de CPU e memória diretamente na gerência do equipamento;

1.1.4.3.7. Deve ser possível realizar a configuração do cluster diretamente na gerência do equipamento. Deve ser possível conectar a serviços de DONS;

1.1.4.3.8. Deve ser possível configurar o timeout da sessão do administrador na interface web.

1.1.4.3.9. Deve ser possível configurar a complexidade da senha do administrador e dias para expirar.

1.1.4.3.10. A solução deve ser capaz de trabalhar com identidades de usuários para propósitos de configurações e logs.

1.1.4.3.11. A solução deve possibilitar ao administrador realizar a integração com o AD (Active Directory) através de um assistente de configuração na própria interface gráfica do produto;

1.1.4.3.12. A solução deve identificar usuários das seguintes fontes pelo menos:

1.1.4.3.13. Active Directory: o gateway de segurança deve realizar consulta aos servidores AD para obter infor mação dos usuários;

1.1.4.3.14. Autenticação via navegador: para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador;

1.1.4.3.15. A identificação do usuário registrado no Microsoft Active Directory, deverá ocorrer sem qualquer tipo de agente instalado nos controladores de domínio e estações dos usuários;

1.1.4.3.16. Na integração com o AD, a operação de cadastro deve ser realizada na própria gerência do equipa menta, de maneira simples e sem utilização de scripts de comando;

1.1.4.4. FUNCIONALIDADE DE PREVENÇÃO DE AMEAÇAS

1.1.4.4.1. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS integrados no próprio equipamento sem a necessidade de uso de quaisquer interfaces ou dispositivos externos.

1.1.4.4.2. Deve ser possível agendar para que o mecanismo de inspeção receba e implemente atualizações para os ataques emergentes sem a necessidade de reiniciar o equipamento;

1.1.4.4.3. Deve ser possível realizar a atualização manualmente sem necessidade de internet através da importação do pacote de atualização.

1.1.4.4.4. Deve incluir a habilidade de detectar e bloquear ataques conhecidos, protegendo, pelo menos, os seguintes ataques conhecidos: SQL Injection, ICMP Denial of Service, força bruta, scanning de portas, CIFS Port overflow, Non Compliant DNS, Non Compliant SMTP, Non Compliant CIFS, Non Compliant MS-SQL Server, IKE aggressive Exchange;

1.1.4.4.5. Deve ser capaz de bloquear tráfego SSH em DNS tunneling;

1.1.4.4.6. A solução deverá ser capaz de inspecionar e proteger apenas hosts internos ou

inspecionar todo o tráfego;

1.1.4.4.7. A solução deve proteger contra-ataques do tipo envenenamento de cache DNS (DNS Cache Poisoning);

1.1.4.4.8. A solução deverá possuir pelo menos dois perfis pré-configurados de fábrica para uso imediato e permitir a customização de um perfil;

1.1.4.4.9. Em cada proteção de segurança, devem estar inclusas informações como: categoria, tipo de impacto na ferramenta, severidade, e tipo de ação que a solução irá executar;

1.1.4.4.10. A solução de IPS deve possuir um modo de solução de problemas, que define o uso de perfil de detecção sem modificar as proteções individuais já criadas e customizadas;

1.1.4.4.11. Deve ser possível criar regras de exceção no IPS para que a solução não faça a inspeção de um tráfego específico por pelo menos proteção, origem, destino, serviço ou porta.

1.1.4.4.12. Deve ser possível visualizar a lista de proteções disponíveis no equipamento com os detalhes.

1.1.4.4.13. A solução deve incluir ferramenta própria ou solução de terceiros para mitigar/bloquear a comunicação entre os hosts infectados com bot e operador remoto (command & contrai).

1.1.4.4.14. A solução deve bloquear arquivos potencialmente maliciosos infectados com malware.

1.1.4.4.15. A solução de proteção contra malware e bot deve compartilhar a mesma política para facilitar o gerenciamento.

1.1.4.4.16. A solução de proteção contra malware e bot deve possuir um modo de solução de problemas, que define o uso de perfil de detecção, sem modificar as proteções individuais já criadas e customizadas;

1.1.4.4.17. As proteções devem ser ativadas baseadas em, pelo menos, critério de nível de confiança, ações da proteção e impacto de performance.

1.1.4.4.18. Deve ser possível habilitar a trilha das proteções para não logar, criar um log ou gerar um alerta;

1.1.4.4.19. Deve ser possível criar regras de exceção para que a solução não faça a inspeção de um tráfego específico por escopo, proteção e definir a ação e log para cada uma delas.

1.1.4.4.20. A solução de anti-malware deve suportar protocolos SMTP e POP3, FTP, HTTP em qualquer porta;

1.1.4.4.20. Deve ser possível definir uma política de inspeção para os tipos de arquivos por:

1.1.4.4.21.1. Inspecionar tipos de arquivos conhecidos que contenham malware;

1.1.4.4.21.2. Inspecionar todos os tipos de arquivos;

1.1.4.4.21. Inspecionar tipos de arquivos de famílias específicas;

1.1.4.4.22. Deve bloquear acesso a URLs com malware;

1.1.4.4.23. Deve ser possível customizar a página exibida para o usuário quando a URL contiver um malware e o acesso for bloqueado;

1.1.4.5. PREVENÇÃO DE AMEAÇAS AVANÇADAS

1.1.4.5.1. A solução deve incluir ferramenta própria ou solução de terceiros para proteção de redes contra ameaças desconhecidas em arquivos que são baixados da Internet ou anexados a e-mails.

1.1.4.5.2. A solução deve compartilhar a mesma política da proteção contra vírus e bot para facilitar o gerenciamento.

1.1.4.5.3. A solução deve trabalhar em modo de prevenção e não apenas detecção.

1.1.4.5.4. Deve permitir criar uma lista de exceção de e-mails que não devem ter seus anexos inspecionados;

1.1.4.5.5. Deve permitir criar uma lista de exceção para arquivos que não devem ser inspecionados. A solução deve suportar protocolos SMTP, HTTP em qualquer porta;

1.1.4.5.6. Deve permitir configurar por tipo de arquivo as ações de inspeção ou bypass.

1.1.4.5.7. A solução deve possuir nuvem de inteligência proprietária do fabricante onde seja responsável em atualizar toda a base de segurança dos appliance através de assinaturas

1.1.4.5.8. Implementar detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF com tamanho até 15 Mb.

1.1.4.5.9. Deve permitir configurar como uma emulação em conexão http será tratada, sendo permitida até que a emulação seja concluída ou bloqueada até a emulação ser completa.

1.1.4.6. FILTRO DE CONTEÚDO WEB

1.1.4.6.1. A solução deverá contar com ferramentas de visibilidade e controle de aplicações web e filtro URL integrada no próprio appliance de segurança que permita a criação de políticas de liberação ou bloqueio baseando-se em aplicações web e URL;

1.1.4.6.2. A gerência das políticas de segurança de controle de aplicação e controle de URL's deverá ser realizada na mesma interface web de gerenciamento;

1.1.4.6.3. Deve ser possível configurar com apenas um clique o bloqueio a sites e aplicações que representem um risco de segurança e estão categorizadas como spyware, phishing, botnet, spam, anonymizer ou hacking.

1.1.4.6.4. Deve ser possível configurar com apenas um clique o bloqueio a sites com conteúdo inapropriado como sexo, violência, armas, jogos e álcool.

1.1.4.6.5. Deve configurar regras para permitir ou bloquear aplicações ou páginas da Internet por pelo menos:

1.1.4.6.5.1. Usuário do Aclive Directory

1.1.4.6.5.2. IP

1.1.4.6.5.3. Rede

1.1.4.6.6. Deve ser possível configurar o bloqueio de compartilhamento de arquivos com origem usualmente ilegais como aplicações torrents e peer-to-peer.

1.1.4.6.7. Deve ser possível configurar manualmente o bloqueio de aplicações ou categorias de sites de aplicações indesejadas.

1.1.4.6.8. Deve ainda ser possível adicionar uma URL ou aplicação que não está na base de dados.

1.1.4.6.9. Deve ser possível limitar o consumo de banda de aplicações.

1.1.4.6.10. A base de aplicações deve ser superior a 2900 aplicações, reconhecendo, pelo menos, as seguintes aplicações: bittorrent, gnutella, skype, facebook, linkedin, twitter, gmail, dropbox, whatsapp, etc;

1.1.4.6.11. Deve ser possível realizar a recategorização de uma URL através da gerência do equipamento.

1.1.4.6.12. Deve ser possível customizar e definir a frequência com que serão exibidas as mensagens para os usuários nas seguintes ações:

1.1.4.6.12.1. Aceitar e informar

1.1.4.6.12.2. Bloquear e informar

1.1.4.6.12.3. Perguntar

1.1.4.7. IDENTIFICAÇÃO DE USUÁRIOS

1.1.4.7.1. A solução deve ser capaz de trabalhar com identidades de usuários para propósitos de configurações e logging.

1.1.4.7.2. A solução deve possibilitar ao administrador realizar a integração com o AD através de um assis tente de configuração na própria interface gráfica do produto;

1.1.4.7.3. A solução deve identificar usuários das seguintes fontes:

1.1.4.7.3.1. Active Directory o gateway de segurança deve realizar consulta aos servidores AD para obter informação dos usuários;

1.1.4.7.3.2. Autenticação via navegador para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador;

1.1.4.7.4. A identificação do usuário registrado no Microsoft Active Directory, deverá ocorrer sem qualquer tipo de agente instalado nos controladores de domínio e estações dos usuários;

1.1.4.7.5. Na integração com o AD, a operação de cadastro deve ser realizada na própria interface web de gerência, de maneira simples e sem utilização de scritps de comando;

1.1.4.8. FUNCIONALIDADES DE CONTROLE DE QUALIDADE DE SERVIÇO E SD-WAN

1.1.4.8.1. Suportar a criação de políticas de controle de serviço por:

1.1.4.8.1.1. Endereço de origem, endereço de destino, por porta e por aplicação;

1.1.4.8.2. Disponibilizar estatísticas em tempo real para as políticas de controle;

1.1.4.8.3. A solução deve permitir, por aplicação, o encaminhamento do tráfego para diferentes links de Internet, sejam eles locais ou remotos, deve suportar múltiplos links de acesso como MPLS, Internet Banda Larga, LTE e Satélite.

1.1.4.8.4. Deve possibilitar a utilização de configuração inteligente de acessos WAN IP ativos-ativos sem a necessidade de switch para agregação WAN, ou seja, distribuir o tráfego simultaneamente pelos N acessos conectados e não apenas na configuração dos acessos principal e backup.

1.1.4.8.5. Medir parâmetros de rede jitter, perda de pacotes e latência em tempo real.

1.1.4.8.6. Se houver necessidade de saída internet do ponto remoto, deve ser possível selecionar por tipo de aplicativo

1.1.4.8.7. Deve permitir a comunicação indireta entre localidades por meio de uma topologia “hub and spoke” e "full mesh"

Deve balancear o tráfego de aplicativos em vários links simultaneamente

1.1.4.8.8. Redistribuição do tráfego balanceado, de forma inteligente, tendo em conta o congestionamento da largura de banda, entre os links utilizados, em caso de falhas nestes links, ou de acordo com as políticas de qualidade pré-definidas

1.1.4.8.9. Habilitar a mesma interface WAN para enviar tráfego simultaneamente por meio de túneis IPSec SD-WAN e nativamente fora dos túneis via underlay.

1.1.4.8.10. Habilitar a criação de políticas de negócios para controlar o padrão de redirecionamento de tráfego e aplicar qualidade de serviço

1.1.4.8.11. Suportar políticas inteligentes usando configurações executem redirecionamento automático e imposição de QoS de voz, vídeo e tráfego transacional

1.1.4.8.12. Suportar o redirecionamento do tráfego de internet de pontos remotos para um ponto de internet centralizado, usando políticas por aplicativo

1.1.4.8.13. Redirecionamento condicionado do tráfego de internet em caso de falha do link de internet local ou do link remoto centralizado, utilizando políticas por aplicativo.

1.1.4.8.14. Suporte simultâneo ao redirecionamento do tráfego da Web de alguns aplicativos para a Internet centralizada, outros aplicativos para a Internet local e outros aplicativos para inspeção avançada de segurança na nuvem.

1.1.4.8.15. Implementar o conceito de perfis de configuração e grupos de objetos para automatizar o processo de implementação de políticas em grande escala sem limitação da quantidade de perfis em uso.

1.1.4.8.16. Deve ser capaz de criar um túnel otimizado que proteja os aplicativos TCP e UDP contra jitter e perda de pacotes para garantir desempenho de ponta a ponta para áudio, vídeo e tráfego transacional.

1.1.4.8.17. Usar probes artificiais baseadas em icmp para medir a qualidade da rede percebida pelo tráfego do usuário, medindo no minimo jitter, latência e perda de pacotes.

1.1.4.8.18. Capacidade de realizar agregação de largura de banda automaticamente entre

links de diferentes velocidades, levando em consideração o uso total da largura de banda

de cada link sem causar congestionamento em links de baixa velocidade.

1.1.4.8.20. Habilitar a configuração de backup do link, ou seja, um link de backup só deve ser ativado quando o link principal falhar.

1.1.4.8.21. Implementar um mecanismo de proteção de variação de latência (jitter) mesmo que a degradação esteja em todos os links, para proteger o tráfego em tempo real (voz e vídeo).

1.1.4.8.22. Garantir o desempenho de aplicativos em um cenário de link de transporte duplo quando ambos os links estão degradados simultaneamente

1.1.4.8.23. Possuir um mecanismo de priorização para proteger o tráfego de aplicativos prioritários quando houver congestionamento em pontos remotos

1.1.4.8.24. Deve automatizar o reconhecimento dos melhores níveis de SLA de rede com base no tipo de tráfego seja áudio, vídeo ou transacional.

1.1.4.8.25. O console de gerenciamento deve informar o status operacional das interfaces LAN e WAN

1.1.4.8.26. O console de gerenciamento deve informar o status operacional de cada dispositivo que faz parte da rede para operacionalidade, inclusive informando a versão da política aplicada em cada dispositivo.

1.1.4.8.27. Realizar medições de “Latência”/”Jitter”/”Queda de pacotes” em cada um dos túneis SDWAN independentemente, na direção de transmissão ou recepção

1.1.4.8.28. O Orquestrador pode estar na Nuvem ou até mesmo ser instalado em um servidor dedicado ou virtualizado, utilizando uma máquina virtual

1.1.4.8.29. No caso do Orquestrator estar na nuvem, a administração de atualizações, gerenciamento de alta disponibilidade e hardening do plano de gerenciamento deve ser realizada pelo fabricante da solução.

1.1.4.9. FUNCIONALIDADES DE ACESSO REMOTO

1.1.4.9.1. A solução deve prover acesso seguro encriptado aos usuários remotos através da Internet;

1.1.4.9.2. A solução deve prover conectividade através de um cliente instalado no computador do usuário e através do navegador do usuário com conexão segura (HTTPS).

1.1.4.9.3. Deve suportar pelo menos os seguintes métodos de conexão:

1.1.4.9.3.1. Conexão através de cliente instalado no laptop ou desktop do usuário.

1.1.4.9.3.2. Conexão através de cliente instalado no smartphone e tablets.

1.1.4.9.3.3. Conexão através de navegador com SSL.

1.1.4.9.3.4. Conexão através de cliente nativo Windows L2TP.

1.1.4.9.4. Solução deve suportar alterar a porta padrão 443 para estabelecimento de VPN SSL.

1.1.4.9.5. A solução deve permitir conexão VPN aos seguintes usuários:

1.1.4.9.5.1. Usuários locais na própria base do appliance.

1.1.4.9.5.2. Grupos de usuários locais na própria base do appliance.

1.1.4.9.5.3. Grupos de usuários do Active Directory.

1.1.4.9.5.4. Grupos de usuários Radius.

1.1.4.9.6. A solução deve permitir atribuir um endereço específico para o usuário remoto.

1.1.4.10. FUNCIONALIDADE DE VPN SITE-TO-SITE

1.1.4.10.1. A solução deve prover acesso seguro criptografado entre duas localidades através da Internet;

1.1.4.10.2. A solução deve estabelecer VPN com o site remoto do próprio fabricante ou de terceiros;

1.1.4.10.3. A solução deve suportar autenticação com senha ou certificado;

1.1.4.10.4. Deve suportar, pelo menos, criptografia AES 128 e 256;

1.1.4.10.5. Deve possuir mecanismo para monitorar a saúde do túnel remoto;

1.1.5. ITEM 5 NEXT GENERATION FIREWALL SEDE TIPO 1

1.1.5.1. CARACTERÍSTICAS GERAIS

1.1.5.1.1. É permitido a composição da solução ofertada entre diversos fabricantes, desde que não contemple solução de software livre;

1.1.5.1.2. A solução deverá ser compatível com SNMPv2 e SNMPv3;

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

1.1.5.1.4. A comunicação entre os appliances de segurança e o módulo de gerência deve ser através de meio criptografado;

1.1.5.1.5. Os appliances de segurança devem suportar operar em cluster ativo-ativo e ativo-passivo sem a necessidade de licenças adicionais;

1.1.5.1.6. Não serão aceitos modelos em listas de end-of-sale, cuja data do fim de vendas seja anterior à data da proposta.

1.1.5.1.7. Não serão aceitos modelos em lista de end-of-support, cuja data do fim do suporte seja anterior ao fim da vigência do contrato e/ou do fim do período de garantia e suporte exigido no edital.

1.1.5.2. CAPACIDADE E QUANTIDADES

1.1.5.2.1. Throughput de, no mínimo, 750 Mbps, com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação, anti-malware e prevenção de ameaças avançadas (dia zero) habilitados simultaneamente;

1.1.5.2.2. Suporte a, no mínimo, 1.900.000 (um milhão e novecentas mil) conexões ou sessões

simultâneas;

1.1.5.2.3. Suporte a, no mínimo, 30.000 (trinta mil) novas conexões ou sessões por segundo;

1.1.5.2.4. Throughput de, no mínimo, 2.5 Gbps (dois ponto cinco), para conexões VPN;

1.1.5.2.5. Armazenamento de, no mínimo, 200GB SSD;

1.1.5.2.6. No mínimo, 5 (cinco) interfaces de rede 1Gbps UTP;

1.1.5.2.7. 1 (uma) interface de rede dedicada ao gerenciamento;

1.1.5.2.8. 1 (uma) interface do tipo console ou similar;

1.1.5.2.9. A solução deve possuir mecanismo para dedicar processamento no equipamento de segurança para funções e ações de gerenciamento, mesmo que o equipamento esteja com alto processamento de CPU. Assim evitando a falta de acesso do administrador para qualquer mitigação de problema e aplicação de política para solução de problema. Entre as funções, deve suportar no mínimo: acesso SSH, acesso WEB, alterações de política, comunicação SNMP.

1.1.5.2.10. O Throughput e as interfaces solicitados neste item deverão ser comprovados através de datasheet público na internet. Não serão aceitas declarações de fabricantes informando números de performance e interfaces;

1.1.5.3. FUNCIONALIDADE DE FIREWALL

1.1.5.3.1. A solução deve consistir de appliance de proteção de rede com funcionalidades de proteção de próxima geração;

1.1.5.3.2. 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 técnica;

1.1.5.3.3. O hardware e software que executem as funcionalidades de proteção de rede deve ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

1.1.5.3.4. Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19", incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;

1.1.5.3.5. Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:

1.1.5.3.6. Suporte a, no mínimo, 1024 VLAN Tags 802.1q, agregação de links 802.3ad, policy based routing ou policy based forwarding, roteamento multicast (PIM-SM), DHCP Relay, DHCP Server e Jumbo Frames;

1.1.5.3.7. A solução deve possuir mecanismo onde identifica o volume de conexões que foi trafegada na regra, assim identificando as regras mais utilizadas;

1.1.5.3.8. Deve suportar os seguintes tipos de NAT:

1.1.5.3.9. Nat dinâmico (Many-to-1), Nat estático (1-to-1), Tradução de porta (PAT), NAT de Origem, NAT de Destino e suportar NAT de Origem e NAT de Destino simultaneamente;

1.1.5.3.10. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;

1.1.5.3.11. Deve suportar NAT64 e NAT46;

1.1.5.3.12. Enviar logs para sistemas de monitoração externos, simultaneamente;

1.1.5.3.13. Prover mecanismo contra-ataques de falsificação de endereços (IP Spoofing), através da especificação da interface de rede pela qual uma comunicação deve se originar baseado na topologia. Não sendo aceito soluções que utilizem tabela de roteamento para esta proteção;

1.1.5.3.14. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
1.1.5.3.15. O firewall deve ter a capacidade de operar de forma simultânea em uma única instancia de Firewall, mediante o uso das suas interfaces físicas nos seguintes modos:

transparente, modo sniffer (monitoramento e análise o tráfego de rede), camada 2 (L2) e

camada 3 (L3);

1.1.5.3.16. Para IPv6, deve suportar roteamento estático e dinâmico (OSPF);

1.1.5.3.17. Suportar OSPF graceful restart;

1.1.5.3.18. Autenticação integrada via Kerberos.

1.1.5.3.19. Cada regra deve, obrigatoriamente, funcionar nas versões de endereço IP 4 e 6 sem duplicação da base de objetos e regras;

1.1.5.3.20. Não serão aceitas soluções nas quais as interfaces de origem e destino tenham que ser obrigatoriamente explicitadas ou obrigatoriamente listadas nas configurações de regras;

1.1.5.4. FUNCIONALIDADE DE CONTROLE DE DADOS E FILTRO DE CONTEÚDO WEB

1.1.5.4.1. A solução deverá contar com ferramentas de visibilidade e controle de aplicações WEB e Filtro URL integrada no próprio appliance de segurança que permite a criação de políticas de liberação ou bloqueio baseando-se em aplicações WEB e URL;

1.1.5.4.2. Controle de políticas por usuários, grupos de usuários, IPs e redes;

1.1.5.4.3. Deve de-criptografar tráfego de entrada e saída em conexões negociadas com TLS 1.2;

1.1.5.4.4. Será aceito soluções de outros fabricantes diferentes do firewall ofertado pela licitante desde que atendido todos os requisitos desta especificação;

1.1.5.4.5. Suportar a atribuição de agendamento às políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

1.1.5.4.6. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:

1.1.5.4.7. Deve ser possível a liberação e bloqueio de aplicações sem a necessidade de liberação de portas e protocolos;

1.1.5.4.8. Reconhecer pelo menos 3.000 (Três mil) aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áu dio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

1.1.5.4.9. Para tráfego criptografado (SSL), deve de-criptografar pacotes a fim de possibilitar a leitura do pay load para checagem de assinaturas de aplicações conhecidas;

1.1.5.4.10. A solução deve suportar a recategorização de URLs local;

1.1.5.4.11. Atualizar a base de assinaturas de aplicações automaticamente;

1.1.5.4.12. A solução deve permitir a solicitação da contratada com o fabricante para categorização de URL na base do fabricante;

1.1.5.4.13. Limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD;

1.1.5.4.14. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no controlador de do mínio, nem nas estações dos usuários;

1.1.5.4.15. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos ou análise heurística;

1.1.5.4.16. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão;

1.1.5.4.17. A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:

1.1.5.4.17.1. Permitir especificar política por tempo, com definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

1.1.5.4.17.2. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes;

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

1.1.5.4.17.4. Deve bloquear o acesso a sites com conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, mesmo que a opção "Safe Search" esteja desabilitada no navegador do usuário;

1.1.5.4.17.5. Suportar base ou cache de URLs local no appliance, çlevitando atrasos de comunicação e validação das URLs. Caso a solução ofertada não suporte localmente, será aceito produto externo desde que não seja so lução de software livre;

1.1.5.4.17.6. Suportar a criação de categorias de URLs customizadas;

1.1.5.4.17.7. Permitir a customização de página de bloqueio;

1.1.5.4.18. Como melhor pratica do uso do acesso a internet e respeitando as políticas de segurança do orgão, a ferramenta deve criar uma pagina customizada ou pop-up onde o usuário será questionado ou informado no momento do acesso a uma pagina URL ou applicação WEB de acordo com as politicas de acesso estabeleci das pela area de TI;

1.1.5.4.19. Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via Radius, para a identificação de endereços IP e usuários;

1.1.5.4.20. 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);

1.1.5.4.21. A solução de controle de dados deve trazer de fábrica vários tipos de arquivos reconhecidos nativamente, permitindo a reconhecimento de pelo menos os seguintes tipos de dados e arquivos:

1.1.5.4.21.1. PCI números de cartão de crédito;

1.1.5.4.21.2. Arquivos PDF;

1.1.5.4.21.3. Arquivos executáveis;

1.1.5.4.21.4. Arquivos de banco de dados;

1.1.5.4.21.5. Arquivos do tipo documento;

1.1.5.4.21.6. Arquivos do tipo apresentação;

1.1.5.4.21.7. Arquivos do tipo planil ha;

1.1.5.4.21.8. A solução de controle de dados deve permitir que as direções do tráfego inspecionado sejam defini das no momento da criação da politica, tais como: "Upload", "Download" e "Download e Upload".

1.1.5.4.22. A solução de controle de dados deve permitir que o usuário receba uma notificação, redirect de uma página web, sempre que um arquivo reconhecido por match em uma regra em uma das categorias acima, seja feito.

1.1.5.4.23. A solução de controle de dados deve permitir, inspecionar e prevenir vazamentos de

arquivos mesmo quando estes estes sendo trafegados pela Web em páginas utilizando o protocolo HTTPS.

1.1.5.5. FUNCIONALIDADES DE PREVENÇÃO DE AMEAÇAS

1.1.5.5.1. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS e suportar os módulos de: Antivírus e Anti-Malware integrados no próprio equipamento de firewall;

1.1.5.5.2. Possuir capacidade de detecção de, no mínimo, 7.000 (sete mil) assinaturas de ataques pré-definidos;

1.1.5.5.3. A solução deve sincronizar ou aplicar as assinaturas de IPS, Antivírus, Anti- Malware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;

1.1.5.5.4. A fim de não criar indisponibilidade no appliance de segurança, a solução de IPS deve possuir mecanismo de fail-open baseado em software, configurável baseado em thresholds de CPU e memória do dispositivo;

1.1.5.5.5. Deve suportar granularidade nas políticas de 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;

1.1.5.5.6. A solução de IPS deve possuir análise de padrões de estado de conexões, análise de decodifica ção de protocolo, análise para detecção de anomalias de protocolo, remontagem de pacotes de TCP e bloqueio de pacotes malformados;

1.1.5.5.7. Detectar e bloquear a origem de portscans;

1.1.5.5.8. Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaluras e customizações;

1.1.5.5.9. A solução de IPS, deve suportar a inclusão de novas assinaturas e customização no formato SNORT;

1.1.5.5.10. Possuir assinaturas para bloqueio de ataques de buffer overflow;

1.1.5.5.11. Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP;

1.1.5.5.12. Suportar bloqueio de arquivos por tipo;

1.1.5.5.13. Identificar e bloquear comunicação com botnets;

1.1.5.5.14. Deve suportar referência cruzada com CVE;

1.1.5.5.15. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:

1.1.5.5.16. O nome da assinatura e do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo de proteção;

1.1.5.5.17. Deve suportar a captura de pacotes (PCAP), em assinatura de IPS e Anti-Malware, através da console de gerência centralizada;

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

1.1.5.5.19. Deve suportar a inspeção em arquivos comprimidos (zip, gzip,etc.);

1.1.5.5.20. Possuir a capacidade de prevenção de ameaças não conhecidas;

1.1.5.5.21. Suportar a criação de políticas por Geo Localização, permitindo que o tráfego de determinado País/ Países seja bloqueado;

1.1.5.5.22. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

1.1.5.5.23. A solução de anti-malware, deve ser capaz de detectar e bloquear ações de callbacks;

1.1.5.6. FUNCIONALIDADES DE CONTROLE DE QUALIDADE DE SERVIÇO

1.1.5.6.1. Suportar a criação de políticas de QoS por:

1.1.5.6.2. Endereço de origem, endereço de destino e por porta;

1.1.5.6.3. O QoS deve possibilitar a definição de classes por:

1.1.5.6.4. Banda garantida;

1.1.5.6.5. Banda máxima ;

1.1.5.6.6. Fila de prioridade;

1.1.5.6.7. Disponibilizar estatísticas RealTime para classes de QoS;

1.1.5.7. FUNCIONALIDADES DE VPN

1.1.5.7.1. Suportar VPN Site-to-Site e Cliente-To-Site;

1.1.5.7.2. Suportar IPSec VPN;

1.1.5.7.3. Suportar SSL VPN;

1.1.5.7.4. A VPN IPSEc deve suportar:

1.1.5.7.4.1. 3DES, Autenticação MOS e SHA-1, Diffie-Hellman Group 1, Group 2, Group 5 e Group 14, Algoritmo Internet Key Exchange (IKE), AES 128 e 256 (Advanced Encryption Standard) e Autenticação via certificado IKE PKI;

1.1.5.7.5. A solução deve suportar CA Interna e CA Externa de terceiros;

1.1.5.7.6. Solução deve suportar a configuração VPN através de uma interface do tipo GUI (console do fabri cante ou interface web);

1.1.5.8. SOLUÇÃO DE PROTEÇÃO CONTRA AMEAÇAS AVANÇADAS

1.1.5.8.1. A solução deverá prover as funcionalidades de inspeção de artefatos de entrada com malwares não conhecidos ou do tipo APT com filtro de ameaças avançadas e análise de execução em tempo real, sendo essa analise executada na nuvem proprietária da própria fabricante ou appliance dedicada para sandboxing;

1.1.5.8.2. Prevenir através do bloqueio efetivo do malware desconhecido (Dia Zero), oriundo da comunicação Web (HTTP e HTTPS) e E-mail (SMTP/TLS) via MTA durante análise completa do arquivo no ambiente sandbox, sem que o mesmo seja entregue parcialmente ao cliente.

1.1.5.8.3. A solução deve ser capaz de inspecionar e prevenir malware desconhecido em tráfego criptografado SSL;

1.1.5.8.4. A solução deve fornecer a capacidade de emular ataques em diferentes sistemas operacionais, dentre eles: Windows 7, Windows 8.1 e Windows 10, assim como Office 2003, 2010, 2013 e 2016;

1.1.5.8.5. Implementar atualização da base de dados de forma automática, permitindo agendamentos diários, dias da semana ou dias do mês assim como o período de cada atualização;

1.1.5.8.6. A solução deve suportar as seguintes topologias de implantação: Inline, Message Transfer Agent (MTA) e Mirrar/TAP;

1.1.5.8.7. A tecnologia de máquina virtual deverá possuir diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso, não sendo baseado apenas em assinaturas;

1.1.5.8.8. A solução de prevenção de ameaças avançadas (Sandboxing) contra ataques persistentes e ZeroDay, deve ser habilitada e funcionar de forma independente, ou seja, não sendo obrigatório o uso e ativação de funcionalidades ou engines de antivírus para a mesma ter o

seu devido funcionamento.

1.1.5.8.9. Todas as máquinas virtuais (Windows e pacote Office) utilizadas na solução e solicitadas neste edital, devem estar integralmente instaladas e licenciadas, sem a necessidade de intervenções por parte do administrador do sistema. As atualizações deverão ser providas pelo fabricante;

1.1.5.8.10. Para a emulação de arquivos, a solução deve suportar arquivos com tamanho máximo de emulação de até 30Mb.

1.1.5.8.11. Implementar mecanismo de exceção, permitindo a criação de regras por VLAN, subrede e endereço IP;

1.1.5.8.12. Implementar a emulação, detecção e bloqueio de qualquer malware e/ou código malicioso detecta do como desconhecido. A solução deve permitir a análise e bloqueio dos seguintes tipos de arquivos caso tenham malware desconhecido: pdf, tar, zip, rar, 7z, exe, rtf, csv, ser, xls, xlsx, xlt, xlm, xltx, xlsm, xltm, xlsb, xla, xlam, xll, xlw, ppt, pptx, pps, pptm, potx, potm, ppam, ppsx, ppsm, doe, docx, dot, doem, dotx, dotm;

1.1.5.8.13. A solução deve permitir a criação de Whitelists baseado no MD5 do arquivo;

1.1.5.8.14. Para melhor administração da solução, a solução deve possibilitar as seguintes

visualizações a nível de monitoração:

1.1.5.8.14.1. Quantidade de arquivos que estão em emulação;

1.1.5.8.14.2. Número de arquivos emulados;

1.1.5.8.15. A solução deve possuir os indicadores abaixo referente ao último dia, última semana ou últimos 30 dias:

1.1.5.8.15.1. Arquivos scaneados;

1.1.5.8.15.2. Arquivos maliciosos;

1.1.6. ITEM 6 NEXT GENERATION FIREWALL SEDE TIPO II

1.1.6.1. CARACTERÍSTICAS GERAIS

1.1.6.1.1. É permitido a composição da solução ofertada entre diversos fabricantes, desde que não contemple solução de software livre;

1.1.6.1.2. A solução deverá ser compatível com SNMPv2 e SNMPv3;

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

1.1.6.1.4. A comunicação entre os appliances de segurança e o módulo de gerência deve ser através de meio criptografado;

1.1.6.1.5. Os appliances de segurança devem suportar operar em cluster ativo-ativo e ativo-passivo sem a necessidade de licenças adicionais;

1.1.6.1.6. Não serão aceitos modelos em listas de end-of-sale, cuja data do fim de vendas seja anterior à data da proposta.

1.1.6.1.7. Não serão aceitos modelos em lista de end-of-support, cuja data do fim do suporte seja anterior ao fim da vigência do contrato e/ou do fim do período de garantia e suporte exigido no edital.

1.1.6.2. CAPACIDADE E QUANTIDADES

1.1.6.2.1. Throughput de, no mínimo, 4.7 Gbps, com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação, anti-malware e prevenção de ameaças avançadas (dia zero)

habilitados simultaneamente;

1.1.6.2.2. Suporte a, no mínimo, 7.000.000 (sete milhões) de conexões ou sessões simultâneas;

1.1.6.2.3. Suporte a, no mínimo, 175.000 (cento e setenta e cinco mil) novas conexões ou sessões por segundo;

1.1.6.2.4. Throughput de, no mínimo, 18 Gbps (dezoito), para conexões VPN;

1.1.6.2.5. Armazenamento de, no mínimo, 400GB SSD;

1.1.6.2.6. Possuir, no mínimo, 8 (oito) interfaces de rede 1Gbps UTP;

1.1.6.2.7. Possuir, no mínimo, 6 (seis) interfaces de rede 10 Gbps SFP+;

1.1.6.2.8. Capacidade para suportar, pelo menos, 12 contextos virtuais;

1.1.6.2.9. Possuir fonte de alimentação redundante;

1.1.6.2.10. Possuir 1 (uma) interface de rede dedicada ao gerenciamento;

1.1.6.2.11. Possuir 1 (uma) interface de rede dedicada para sincronismo;

1.1.6.2.12. Possuir 1 (uma) interface do tipo console ou similar;

1.1.6.2.13. Possuir interface dedicada e física para gerenciamento do equipamento fora de banda. Essa interface deve ser um canal de gerenciamento que funcione mesmo quando o dispositivo é desligado ou não responde. Caso o equipamento não possua essa interface tisica/dedicada, deverá ser composta com outro equipamento de terceiro onde faça essa função. Não sendo permitido qualquer tipo de configuração de instâncias via software.

1.1.6.2.14. A solução deve possuir mecanismo para dedicar processamento no equipamento de segurança para funções e ações de gerenciamento, mesmo que o equipamento esteja com alto processamento de CPU. Assim evitando a falta de acesso do administrador para qualquer mitigação de problema e aplicação de política para solução de problema. Entre as funções, deve suportar no mínimo: acesso SSH, acesso WEB, alterações de política, comunicação SNMP.

1.1.6.2.15. O Throughput e as interfaces solicitados neste item deverão ser comprovados através de datasheet público na internet. Não serão aceitas declarações de fabricantes informando números de performance e interfaces;

1.1.6.3. FUNCIONALIDADE DE FIREWALL

1.1.6.3.1. A solução deve consistir de appliance de proteção de rede com funcionalidades de proteção de próxima geração;

1.1.6.3.2. 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 técnica;

1.1.6.3.3. O hardware e software que executem as funcionalidades de proteção de rede deve ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

1.1.6.3.4. Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19", incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;

1.1.6.3.5. Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:

1.1.6.3.6. Suporte a, no mínimo, 1024 VLAN Tags 802.1q, agregação de links 802.3ad, policy based routing ou policy based forwarding, roteamento multicast (PIM-SM), DHCP Relay, DHCP Server e Jumbo Frames;

1.1.6.3.7. A solução deve possuir mecanismo onde identifica o volume de conexões que foi trafegada na regra, assim identificando as regras mais utilizadas;

1.1.6.3.8. Deve suportar os seguintes tipos de NAT:

1.1.6.3.9. Nat dinâmico (Many-to-1), Nat estático (1-to-1), Tradução de porta (PAT), NAT de Origem, NAT de Destino e suportar NAT de Origem e NAT de Destino simultaneamente;

1.1.6.3.10. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;

1.1.6.3.11. Deve suportar NAT64 e NAT46;

1.1.6.3.12. Enviar logs para sistemas de monitoração externos, simultaneamente;

1.1.6.3.13. Prover mecanismo contra-ataques de falsificação de endereços (IP Spoofing), através da especificação da interface de rede pela qual uma comunicação deve se originar baseado na topologia. Não sendo aceito soluções que utilizem tabela de roteamento para esta proteção;

1.1.6.3.14. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
1.1.6.3.15. O firewall deve ter a capacidade de operar de forma simultânea em uma única instancia de Firewall, mediante o uso das suas interfaces físicas nos seguintes modos:

transparente, modo sniffer (monitoramento e análise o tráfego de rede), camada 2 (L2) e

camada 3 (L3);

1.1.6.3.16. Para IPv6, deve suportar roteamento estático e dinâmico (OSPF);

1.1.6.3.17. Suportar OSPF graceful restart;

1.1.6.3.18. Autenticação integrada via Kerberos.

1.1.6.3.19. Cada regra deve, obrigatoriamente, funcionar nas versões de endereço IP 4 e 6 sem duplicação da base de objetos e regras;

1.1.6.3.20. Não serão aceitas soluções nas quais as interfaces de origem e destino tenham que ser obrigatoriamente explicitadas ou obrigatoriamente listadas nas configurações de regras;

1.1.6.4. FUNCIONALIDADE DE CONTROLE DE DADOS E FILTRO DE CONTEÚDO WEB

1.1.6.4.1. A solução deverá contar com ferramentas de visibilidade e controle de aplicações WEB e Filtro URL integrada no próprio appliance de segurança que permite a criação de políticas de liberação ou bloqueio baseando-se em aplicações WEB e URL;

1.1.6.4.2. Controle de políticas por usuários, grupos de usuários, IPs e redes;

1.1.6.4.3. Deve de-criptografar tráfego de entrada e saída em conexões negociadas com TLS 1.2;

1.1.6.4.4. Será aceito soluções de outros fabricantes diferentes do firewall ofertado pela licitante desde que atendido todos os requisitos desta especificação;

1.1.6.4.5. Suportar a atribuição de agendamento às políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

1.1.6.4.6. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:

1.1.6.4.7. Deve ser possível a liberação e bloqueio de aplicações sem a necessidade de liberação de portas e protocolos;

1.1.6.4.8. Reconhecer pelo menos 3.000 (Três mil) aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

1.1.6.4.9. Para tráfego criptografado (SSL), deve de-criptografar pacotes a fim de possibilitar a leitura do pay load para checagem de assinaturas de aplicações conhecidas;

1.1.6.4.10. A solução deve suportar a recategorização de URLs local;

1.1.6.4.11. Atualizar a base de assinaturas de aplicações automaticamente;

1.1.6.4.12. A solução deve permitir a solicitação da contratada com o fabricante para categorização de URL na base do fabricante;

1.1.6.4.13. Limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD;

1.1.6.4.14. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Aclive Directory, sem a necessidade de instalação de agente no controlador de do mínio, nem nas estações dos usuários;

1.1.6.4.15. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos ou análise heurística;

1.1.6.4.16. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão;

1.1.6.4.17. A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:

1.1.6.4.17.1. Permitir especificar política por tempo, com definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

1.1.6.4.17.2. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes;

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

1.1.6.4.17.4. Deve bloquear o acesso a sites com conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, mesmo que a opção "Safe Search" esteja desabilitada no navegador do usuário;

1.1.6.4.17.5. Suportar base ou cache de URLs local no appliance, evitando atrasos de comunicação e validação das URLs. Caso a solução ofertada não suporte localmente, será aceito produto externo desde que não seja solução de software livre;

1.1.6.4.17.6. Suportar a criação de categorias de URLs customizadas;

1.1.6.4.17.7. Permitir a customização de página de bloqueio;

1.1.6.4.18. Como melhor prática do uso do acesso a internet e respeitando as políticas de segurança do orgão, a ferramenta deve criar uma página customizada ou pop-up onde o usuário será questionado ou informado no momento do acesso a uma página URL ou applicação WEB de acordo com as políticas de acesso estabelecidas pela área de TI;

1.1.6.4.19. Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via Radius, para a identificação de endereços IP e usuários;

1.1.6.4.20. 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);

1.1.6.4.21. A solução de controle de dados deve trazer de fábrica vários tipos de arquivos reconhecidos nativamente, permitindo a reconhecimento de pelo menos os seguintes tipos de dados e arquivos:

1.1.6.4.21.1. PCI números de cartão de crédito;

1.1.6.4.21.2. Arquivos PDF;

1.1.6.4.21.3. Arquivos executáveis;

1.1.6.4.21.4. Arquivos de banco de dados;

1.1.6.4.21.5. Arquivos do tipo documento;

1.1.6.4.21.6. Arquivos do tipo apresentação;

1.1.6.4.21.7. Arquivos do tipo planilha;

1.1.6.4.22. A solução de controle de dados deve permitir que as direções do tráfego inspecionado sejam defini das no momento da criação da politica, tais como: "Upload", "Download" e "Download e Upload".

1.1.6.4.23. A solução de controle de dados deve permitir que o usuário receba uma notificação, redirect de uma página web, sempre que um arquivo reconhecido por match em uma regra em uma das categorias acima, seja feito.

1.1.6.4.24. A solução de controle de dados deve permitir, inspecionar e prevenir vazamentos de arquivos mesmo quando estes estes sendo trafegados pela Web em páginas utilizando o protocolo HTTPS.

1.1.6.5. FUNCIONALIDADES DE PREVENÇÃO DE AMEAÇAS

1.1.6.5.1. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS e suportar os módulos de: Antivírus e Anti-Malware integrados no próprio equipamento de firewall;

1.1.6.5.2. Possuir capacidade de detecção de, no mínimo, 7.000 (sete mil) assinaturas de ataques pré-defini dos;

1.1.6.5.3. A solução deve sincronizar ou aplicar as assinaturas de IPS, Antivírus, Anti- Malware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;

1.1.6.5.4. A fim de não criar indisponibilidade no appliance de segurança, a solução de IPS deve possuir mecanismo de fail-open baseado em software, configurável baseado em thresholds de CPU e memória do dispositivo;

1.1.6.5.5. Deve suportar granularidade nas políticas de 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;

1.1.6.5.6. A solução de IPS deve possuir análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, remontagem de pacotes de TCP e bloqueio de pacotes malformados;

1.1.6.5.7. Detectar e bloquear a origem de portscans;

1.1.6.5.8. Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações;

1.1.6.5.9. A solução de IPS, deve suportar a inclusão de novas assinaturas e customização no formato SNORT;

1.1.6.5.10. Possuir assinaturas para bloqueio de ataques de buffer overflow;

1.1.6.5.11. Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP;

1.1.6.5.12. Suportar bloqueio de arquivos por tipo;

1.1.6.5.13. Identificar e bloquear comunicação com botnets;

1.1.6.5.14. Deve suportar referência cruzada com CVE;

1.1.6.5.15. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:

1.1.6.5.16. O nome da assinatura e do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo de proteção;

1.1.6.5.17. Deve suportar a captura de pacotes (PCAP), em assinatura de IPS e Anti-Malware, através da console de gerência centralizada;

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

1.1.6.5.19. Deve suportar a inspeção em arquivos comprimidos (zip, gzip,etc.);

1.1.6.5.20. Possuir a capacidade de prevenção de ameaças não conhecidas;

1.1.6.5.21. Suportar a criação de políticas por Geo Localização, permitindo que o tráfego de determinado País/ Países seja bloqueado;

1.1.6.5.22. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

1.1.6.5.23. A solução de anti-malware, deve ser capaz de detectar e bloquear ações de callbacks;

1.1.6.6. FUNCIONALIDADES DE CONTROLE DE QUALIDADE DE SERVIÇO

1.1.6.6.1. Suportar a criação de políticas de QoS por:

1.1.6.6.2. Endereço de origem, endereço de destino e por porta;

1.1.6.6.3. O QoS deve possibilitar a definição de classes por:

1.1.6.6.4. Banda garantida;

1.1.6.6.5. Banda máxima ;

1.1.6.6.6. Fila de prioridade;

1.1.6.6.7. Disponibilizar estatísticas RealTime para classes de QoS;

1.1.6.7. FUNCIONALIDADES DE VPN

1.1.6.7.1. Suportar VPN Site-to-Site e Cliente-To-Site;

1.1.6.7.2. Suportar IPSec VPN;

1.1.6.7.3. Suportar SSL VPN;

1.1.6.7.4. A VPN IPSEc deve suportar:

1.1.6.7.4.1. 3DES, Autenticação MOS e SHA-1, Diffie-Hellman Group 1, Group 2, Group 5 e Group 14, Algoritmo Internet Key Exchange (IKE), AES 128 e 256 (Advanced Encryption Standard) e Autenticação via certificado IKE PKI;

1.1.6.7.5. A solução deve suportar CA Interna e CA Externa de terceiros;

1.1.6.7.6. Solução deve suportar a configuração VPN através de uma interface do tipo GUI (console do fabricante ou interface web);

1.1.6.8. SOLUÇÃO DE PROTEÇÃO CONTRA AMEAÇAS AVANÇADAS

1.1.6.8.1. A solução deverá prover as funcionalidades de inspeção de artefatos de entrada com malwares não conhecidos ou do tipo APT com filtro de ameaças avançadas e análise de execução em tempo real, sendo essa análise executada na nuvem proprietária do próprio fabricante ou appliance dedicada para sandboxing;

1.1.6.8.2. Prevenir através do bloqueio efetivo do malware desconhecido (Dia Zero), oriundo da comunicação Web (HTTP e HTTPS) e E-mail (SMTP/TLS) via MTA durante análise completa do arquivo no ambiente sandbox, sem que o mesmo seja entregue parcialmente ao cliente.

1.1.6.8.3. A solução deve ser capaz de inspecionar e prevenir malware desconhecido em tráfego criptografado SSL;

1.1.6.8.4. A solução deve fornecer a capacidade de emular ataques em diferentes sistemas operacionais, dentre eles: Windows 7, Windows 8.1 e Windows 10, assim como Office 2003, 2010, 2013 e 2016;

1.1.6.8.5. Implementar atualização da base de dados de forma automática, permitindo agendamentos diários, dias da semana ou dias do mês assim como o período de cada atualização;

1.1.6.8.6. A solução deve suportar as seguintes topologias de implantação: Inline, Message Transfer Agent

1.1.6.8.7. (MTA) e Mirrar/TAP;

1.1.6.8.8. A tecnologia de máquina virtual deverá possuir diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso, não sendo baseado apenas em assinaturas;

1.1.6.8.9. A solução de prevença de ameaças avançadas (Sandboxing) contra-ataques persistentes e ZeroDay, deve ser habilitada e funcionar de forma independente, ou seja, não sendo obrigatório o uso e ativação de funcionalidades ou engines de antivírus para a mesma ter o seu devido funcionamento.

1.1.6.8.10. Todas as máquinas virtuais (Windows e pacote Office) utilizadas na solução e solicitadas neste edital, devem estar integralmente instaladas e licenciadas, sem a necessidade de intervenções por parte do administrador do sistema. As atualizações deverão ser providas pelo fabricante;

1.1.6.8.11. Para a emulação de arquivos, a solução deve suportar arquivos com tamanho máximo de emulação de até 30Mb.

1.1.6.8.12. Implementar mecanismo de exceção, permitindo a criação de regras por VLAN, subrede e endereço IP;

1.1.6.8.13. Implementar a emulação, detecção e bloqueio de qualquer malware e/ou código malicioso detecta do como desconhecido. A solução deve permitir a análise e bloqueio dos seguintes tipos de arquivos caso tenham malware desconhecido: pdf, tar, zip, rar, 7z, exe, rtf, csv, ser, xls, xlsx, xlt, xlm, xltx, xlsm, xltm, xlsb, xla, xlam, xll, xlw, ppt, pptx, pps, pptm, potx, potm, ppam, ppsx, ppsm, doe, docx, dot, doem, dotx, dotm;

1.1.6.8.14. A solução deve permitir a criação de Whitelists baseado no MD5 do arquivo;

1.1.6.8.15. Para melhor administração da solução, a solução deve possibilitar as seguintes

visualizações a nível de monitoração:

1.1.6.8.15.1. Quantidade de arquivos que estão em emulação;

1.6.8.14.2. Número de arquivos emulados;

1.1.6.8.15.2. A solução deve possuir os indicadores abaixo referente ao último dia, última semana ou últimos 30 dias:

1.1.6.8.15.2.1. Arquivos scaneados;

1.1.6.8.15.2.2. Arquivos maliciosos;

1.1.7. ITEM 7 NEXT GENERATION FIREWALL SEDE TIPO III

1.1.7.1. CARACTERÍSTICAS GERAIS

1.1.7.1.1. É permitido a composição da solução ofertada entre diversos fabricantes, desde que não contem pela solução de software livre;

1.1.7.1.2. A solução deverá ser compatível com SNMPv2 e SNMPv3;

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

1.1.7.1.4. A comunicação entre os appliances de segurança e o módulo de gerência deve ser através de meio criptografado;

1.1.7.1.5. Os appliances de segurança devem suportar operar em cluster ativo-ativo e ativo-passivo sem a necessidade de licenças adicionais;

1.1.7.1.6. Não serão aceitos modelos em listas de end-of-sale, cuja data do fim de vendas seja anterior à data da proposta.

1.1.7.1.7. Não serão aceitos modelos em lista de end-of-support, cuja data do fim do suporte seja anterior ao fim da vigência do contrato e/ou do fim do período de garantia e suporte exigido no edital.

1.1.7.2. CAPACIDADE E QUANTIDADES

1.1.7.2.1. Throughput de, no mínimo, 8 Gbps, com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação, anti-malware e prevenção de ameaças avançadas (dia zero) habilitados simultaneamente;

1.1.7.2.2. Suporte a, no mínimo, 7.000.000 (sete milhões) de conexões ou sessões simultâneas;

1.1.7.2.3. Suporte a, no mínimo, 290.000 (duzentas e noventa mil) novas conexões ou sessões por segundo;

1.1.7.2.4.

1.1.7.2.5. Throughput de, no mínimo, 30 Gbps (trinta) para conexões VPN;

1.1.7.2.6. Armazenamento de, no mínimo, 400GB SSD;

1.1.7.2.7. Possuir, no mínimo, 8 (oito) interfaces de rede 1Gbps UTP;

1.1.7.2.8. Possuir, no mínimo, 6 (seis) interfaces de rede 10 Gbps SFP+;

1.1.7.2.9. Capacidade para suportar, pelo menos, 12 contextos virtuais;

1.1.7.2.10. Possuir fonte de alimentação redundante;

1.1.7.2.11. Possuir 1 (uma) interface de rede dedicada ao gerenciamento;

1.1.7.2.12. Possuir 1 (uma) interface de rede dedicada para sincronismo;

1.1.7.2.13. Possuir 1 (uma) interface do tipo console ou similar;

1.1.7.2.14. Possuir interface dedicada e física para gerenciamento do equipamento fora de banda. Essa interface deve ser um canal de gerenciamento que funcione mesmo quando o dispositivo é desligado ou não responde. Caso o equipamento não possua essa interface tisica/dedicada, deverá ser composta com outro equipa mento de terceiro onde faça essa função. Não sendo permitido qualquer tipo de configuração de instancias via software.

1.1.7.2.15. A solução deve possuir mecanismo para dedicar processamento no equipamento de segurança para funções e ações de gerenciamento, mesmo que o equipamento esteja com alto processamento de CPU. Assim evitando a falta de acesso do administrador para qualquer mitigação de problema e aplicação de política para solução de problema. Entre as funções, deve suportar no mínimo: acesso SSH, acesso WEB, alterações de política, comunicação SNMP.

1.1.7.2.16. O Throughput e as interfaces solicitados neste item deverão ser comprovados através de datasheet público na internet. Não serão aceitas declarações de fabricantes informando números de performance e interfaces;

1.1.7.3. FUNCIONALIDADE DE FIREWALL

1.1.7.3.1. A solução deve consistir de appliance de proteção de rede com funcionalidades de proteção de próxima geração;

1.1.7.3.2. 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 técnica;

1.1.7.3.3. O hardware e software que executem as funcionalidades de proteção de rede deve ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

1.1.7.3.4. Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19", incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;

1.1.7.3.5. Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:

1.1.7.3.6. Suporte a, no mínimo, 1024 VLAN Tags 802.1q, agregação de links 802.3ad, policy based routing ou policy based forwarding, roteamento multicast (PIM-SM), DHCP Relay, DHCP Server e Jumbo Frames;

1.1.7.3.7. A solução deve possuir mecanismo onde identifica o volume de conexões que foi trafegada na regra, assim identificando as regras mais utilizadas;

1.1.7.3.8. Deve suportar os seguintes tipos de NAT:

1.1.7.3.9. Nat dinâmico (Many-to-1), Nat estático (1-to-1), Tradução de porta (PAT), NAT de Origem, NAT de Destino e suportar NAT de Origem e NAT de Destino simultaneamente;

1.1.7.3.10. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;

1.1.7.3.11. Deve suportar NAT64 e NAT46;

1.1.7.3.12. Enviar logs para sistemas de monitoração externos, simultaneamente;

1.1.7.3.13. Prover mecanismo contra ataques de falsificação de endereços (IP Spoofing), através da especificação da interface de rede pela qual uma comunicação deve se originar baseado na topologia. Não sendo aceito soluções que utilizem tabela de roteamento para esta proteção;

1.1.7.3.14. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
1.1.7.3.15. O firewall deve ter a capacidade de operar de forma simultânea em uma única instancia de Firewall, mediante o uso das suas interfaces físicas nos seguintes modos:

transparente, modo sniffer (monitoramento e análise o tráfego de rede), camada 2 (L2) e

camada 3 (L3);

1.1.7.3.16. Para IPv6, deve suportar roteamento estático e dinâmico (OSPF);

1.1.7.3.17. Suportar OSPF graceful restart;

1.1.7.3.18. Autenticação integrada via Kerberos.

1.1.7.3.19. Cada regra deve, obrigatoriamente, funcionar nas versões de endereço IP 4 e 6 sem duplicação da base de objetos e regras;

1.1.7.3.20. Não serão aceitas soluções nas quais as interfaces de origem e destino tenham que ser obrigatoriamente explicitadas ou obrigatoriamente listadas nas configurações de regras;

1.1.7.4. FUNCIONALIDADE DE CONTROLE DE DADOS E FILTRO DE CONTEÚDO WEB

1.1.7.4.1. A solução deverá contar com ferramentas de visibilidade e controle de aplicações WEB e Filtro URL integrada no próprio appliance de segurança que permite a criação de políticas de liberação ou bloqueio baseando-se em aplicações WEB e URL;

1.1.7.4.2. Controle de políticas por usuários, grupos de usuários, IPs e redes;

1.1.7.4.3. Deve de-criptografar tráfego de entrada e saída em conexões negociadas com TLS 1.2;

1.1.7.4.4. Será aceito soluções de outros fabricantes diferentes do firewall ofertado pela licitante desde que atendido todos os requisitos desta especificação;

1.1.7.4.5. Suportar a atribuição de agendamento às políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

1.1.7.4.6. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:

1.1.7.4.7. Deve ser possível a liberação e bloqueio de aplicações sem a necessidade de liberação de portas e protocolos;

1.1.7.4.8. Reconhecer pelo menos 3.000 (Três mil) aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

1.1.7.4.9. Para tráfego criptografado (SSL), deve decriptografar pacotes a fim de possibilitar a leitura do pay load para checagem de assinaturas de aplicações conhecidas;

1.1.7.4.10. A solução deve suportar a recategorização de URLs local;

1.1.7.4.11. Atualizar a base de assinaturas de aplicações automaticamente;

1.1.7.4.12. A solução deve permitir a solicitação da contratada com o fabricante para categorização de URL na base do fabricante;

1.1.7.4.13. Limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD;

1.1.7.4.14. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários;

1.1.7.4.15. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos ou análise heurística;

1.1.7.4.16. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão;

1.1.7.4.17. A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:

1.1.7.4.18. Permitir especificar política por tempo, com definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

1.1.7.4.19. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes;

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

1.1.7.4.21. Deve bloquear o acesso a sites com conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, mesmo que a opção "Safe Search" esteja desabilitada no navegador do usuário;

1.1.7.4.22. Suportar base ou cache de URLs local no appliance, evitando atrasos de comunicação e validação das URLs. Caso a solução ofertada não suporte localmente, será aceito produto externo desde que não seja solução de software livre;

1.1.7.4.23. Suportar a criação de categorias de URLs customizadas;

1.1.7.4.24. Permitir a customização de página de bloqueio;

1.1.7.4.25. Como melhor prática do uso do acesso a internet e respeitando as políticas de

segurança do órgão, a ferramenta deve criar uma página customizada ou pop-up onde o usuário será questionado ou informado no momento do acesso a uma página URL ou applicação WEB de acordo com as políticas de acesso estabelecidas pela area de TI;

1.1.7.4.26. Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via Radius, para a identificação de endereços IP e usuários;

1.1.7.4.27. 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 Fi rewall (Captive Portal);

1.1.7.4.28. A solução de controle de dados deve trazer de fábrica vários tipos de arquivos reconhecidos nativamente, permitindo a reconhecimento de pelo menos os seguintes tipos de dados e arquivos:

1.1.7.4.28.1. PCI números de cartão de crédito;

1.1.7.4.28.2. Arquivos PDF;

1.1.7.4.28.3. Arquivos executáveis

1.1.7.4.28.4. Arquivos de banco de dados;

1.1.7.4.28.5. Arquivos do tipo documento;

1.1.7.4.28.6. Arquivos do tipo apresentação;

1.1.7.4.28.7. Arquivos do tipo planilha;

1.1.7.4.29. A solução de controle de dados deve permitir que as direções do tráfego inspecionado sejam definidas no momento da criação da politica, tais como: "Upload", "Download" e "Download e Upload".

1.1.7.4.30. A solução de controle de dados deve permir que o usuário receba uma notificação, redirect de uma página web, sempre que um arquivo reconhecido por match em uma regra em uma das categorias acima, seja feito.

1.1.7.4.31. A solução de controle de dados deve permitir, inspecionar e prevenir vazamentos de arquivos mes mo quando estes estes sendo trafegados pela Web em páginas utilizando o protocolo HTTPS.

1.1.7.5. FUNCIONALIDADES DE PREVENÇÃO DE AMEAÇAS

1.1.7.5.1. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS e suportar os módulos de: Antivírus e Anti-Malware integrados no próprio equipamento de firewall;

1.1.7.5.2. Possuir capacidade de detecção de, no mínimo, 7.000 (sete mil) assinaturas de ataques pré-definidos;

1.1.7.5.3. A solução deve sincronizar ou aplicar as assinaturas de IPS, Antivírus, Anti- Malware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;

1.1.7.5.4. A fim de não criar indisponibilidade no appliance de segurança, a solução de IPS deve possuir mecanismo de fail-open baseado em software, configurável baseado em thresholds de CPU e memória do dispositivo;

1.1.7.5.5. Deve suportar granularidade nas políticas de 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;

1.1.7.5.6. A solução de IPS deve possuir análise de padrões de estado de conexões, análise de decodifica ção de protocolo, análise para detecção de anomalias de protocolo, remontagem de pacotes de TCP e bloqueio de pacotes malformados;

1.1.7.5.7. Detectar e bloquear a origem de portscans;

1.1.7.5.8. Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações;

1.1.7.5.9. A solução de IPS, deve suportar a inclusão de novas assinaturas e customização no formato SNORT;

1.1.7.5.10. Possuir assinaturas para bloqueio de ataques de buffer overflow;

1.1.7.5.11. Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP;

1.1.7.5.12. Suportar bloqueio de arquivos por tipo;

1.1.7.5.14. Identificar e bloquear comunicação com botnets;

1.1.7.5.15. Deve suportar referência cruzada com CVE;

1.1.7.5.16. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:

1.1.7.5.17. O nome da assinatura e do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo de proteção;

1.1.7.5.18. Deve suportar a captura de pacotes (PCAP), em assinatura de IPS e Anti-Malware, através da console de gerência centralizada;

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

1.1.7.5.20. Deve suportar a inspeção em arquivos comprimidos (zip, gzip,etc.);

1.1.7.5.21. Possuir a capacidade de prevenção de ameaças não conhecidas;

1.1.7.5.22. Suportar a criação de políticas por Geo Localização, permitindo que o tráfego de determinado País/ Países seja bloqueado;

1.1.7.5.23. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

1.1.7.5.24. A solução de anti-malware, deve ser capaz de detectar e bloquear ações de callbacks;

1.1.7.6. FUNCIONALIDADES DE CONTROLE DE QUALIDADE DE SERVIÇO

1.1.7.6.1. Suportar a criação de políticas de QoS por:

1.1.7.6.2. Endereço de origem, endereço de destino e por porta;

1.1.7.6.3. O QoS deve possibilitar a definição de classes por:

1.1.7.6.4. Banda garantida;

1.1.7.6.5. Banda máxima ;

1.1.7.6.6. Fila de prioridade;

1.1.7.6.7. Disponibilizar estatísticas RealTime para classes de QoS;

1.1.7.7. FUNCIONALIDADES DE VPN

1.1.7.7.1. Suportar VPN Site-to-Site e Cliente-To-Site;

1.1.7.7.2. Suportar IPSec VPN;

1.1.7.7.3. Suportar SSL VPN;

1.1.7.7.4. A VPN IPSEc deve suportar:

1.1.7.7.5. 3DES, Autenticação MOS e SHA-1, Diffie-Hellman Group 1, Group 2, Group 5 e Group 14, Algoritmo Internet Key Exchange (IKE), AES 128 e 256 (Advanced Encryption Standard) e

Autenticação via certificado IKE PKI;

1.1.7.7.6. A solução deve suportar CA Interna e CA Externa de terceiros;

1.1.7.7.7. Solução deve suportar a configuração VPN através de uma interface do tipo GUI (console do fabricante ou interface web);

1.1.7.8. SOLUÇÃO DE PROTEÇÃO CONTRA AMEAÇAS AVANÇADAS

1.1.7.8.1. A solução deverá prover as funcionalidades de inspeção de artefatos de entrada com malwares não conhecidos ou do tipo APT com filtro de ameaças avançadas e análise de execução em tempo real, sendo essa analise executada na nuvem proprietária da próprio fabricante ou appliance dedicada para sandboxing;

1.1.7.8.2. Prevenir através do bloqueio efetivo do malware desconhecido (Dia Zero), oriundo da comunicação Web (HTTP e HTTPS) e E-mail (SMTP/TLS) via MTA durante análise completa do arquivo no ambiente sandbox, sem que o mesmo seja entregue parcialmente ao cliente.

1.1.7.8.3. A solução deve ser capaz de inspecionar e prevenir malware desconhecido em tráfego criptografado SSL;

1.1.7.8.4. A solução deve fornecer a capacidade de emular ataques em diferentes sistemas operacionais, dentre eles: Windows 7, Windows 8.1 e Windows 10, assim como Office 2003, 2010, 2013 e 2016;

1.1.7.8.5. Implementar atualização da base de dados de forma automática, permitindo agendamentos diários, dias da semana ou dias do mês assim como o período de cada atualização;

1.1.7.8.6. A solução deve suportar as seguintes topologias de implantação: Inline, Message Transfer Agent

1.1.7.8.7. (MTA) e Mirror/TAP;

1.1.7.8.8. A tecnologia de máquina virtual deverá possuir diferentes sistemas operacionais, de modo a permi tir a análise completa do comportamento do malware ou código malicioso, não sendo baseado apenas em assinaturas;

1.1.7.8.9. A solução de prevença de ameaças avançadas (Sandboxing) contra ataques persistentes e ZeroDay, deve ser habilitada e funcionar de forma independente, ou seja, não sendo obrigatório o uso e ativação de funcionalidades ou engines de anti-virus para a mesma ter o seu devido funcionamento.

1.1.7.8.10. Todas as máquinas virtuais (Windows e pacote Office) utilizadas na solução e solicitadas neste edital, devem estar integralmente instaladas e licenciadas, sem a necessidade de intervenções por parte do administrador do sistema. As atualizações deverão ser providas pelo fabricante;

1.1.7.8.11. Para a emulação de arquivos, a solução deve suportar arquivos com tamanho máximo de emulação de até 30Mb.

1.1.7.8.12. Implementar mecanismo de exceção, permitindo a criação de regras por VLAN, subrede e endereço IP;

1.1.7.8.13. Implementar a emulação, detecção e bloqueio de qualquer malware e/ou código malicioso detectado como desconhecido. A solução deve permitir a análise e bloqueio dos seguintes tipos de arquivos caso tenham malware desconhecido: pdf, tar, zip, rar, 7z, exe, rtf, csv, ser, xls, xlsx, xlt, xlm, xltx, xlsm, xltm, xlsb, xla, xlam, xll, xlw, ppt, pptx, pps, pptm, potx, potm, ppam, ppsx, ppsm, doe, docx, dot, doem, dotx, dotm;

1.1.7.8.14. A solução deve permitir a criação de Whitelists baseado no MD5 do arquivo;

1.1.7.8.15. Para melhor administração da solução, a solução deve possibilitar as seguintes

visualizações a nível de monitoração:

1.1.7.8.15.1. Quantidade de arquivos que estão em emulação;

1.1.7.8.15.2. Número de arquivos emulados;

1.1.7.8.16. A solução deve possuir os indicadores abaixo eferente ao último dia, última semana ou últimos 30 dias:

1.1.7.8.16.1. Arquivos scaneados;

1.1.7.8.16.2. Arquivos maliciosos;

1.1.8. ITEM 8 NEXT GENERATION FIREWALL DATA CENTER TIPO 1

1.1.8.1. CARACTERÍSTICAS GERAIS

1.1.8.1.1. É permitido a composição da solução ofertada entre diversos fabricantes, desde que não contem ple solução de software livre;

1.1.8.1.2. A solução deverá ser compatível com SNMPv2 e SNMPv3;

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

1.1.8.1.4. A comunicação entre os appliances de segurança e o módulo de gerência deve ser através de meio criptografado;

1.1.8.1.5. Os appliances de segurança devem suportar operar em cluster ativo-ativo e ativo-passivo sem a necessidade de licenças adicionais;

1.1.8.1.6. Não serão aceitos modelos em listas de end-of-sale, cuja data do fim de vendas seja anterior à data da proposta.

1.1.8.1.7. Não serão aceitos modelos em lista de end-of-support, cuja data do fim do suporte seja anterior ao fim da vigência do contrato e/ou do fim do período de garantia e suporte exigido no edital.

1.1.8.2. CAPACIDADE E QUANTIDADES

1.1.8.2.1. Throughput de, no mínimo, 16 Gbps, com as funcionalidades de firewall, prevenção de intrusão,

1.1.8.2.2. controle de aplicação, anti-malware e prevenção de ameaças avançadas (dia zero) habilitados simultaneamente;

1.1.8.2.3. Suporte a, no mínimo, 14.000.000 (quatorze milhões) de conexões ou sessões simultâSuporte a, no mínimo, 520.000 (quinhentos e vinte mil) novas conexões ou sessões por segundo;

1.1.8.2.4. Throughput de, no mínimo, 70 Gbps (setenta), para conexões VPN;

1.1.8.2.5. Armazenamento redundante de, no mínimo, 900 GB SSD ou HDD;

1.1.8.2.6. Possuir, no mínimo, 4 (quatro) interfaces de rede 1Gbps UTP;

1.1.8.2.7. Possuir, no mínimo, 10 (dez) interfaces de rede 10 Gbps SFP+;

1.1.8.2.8. Suportar expansão futura para, no mínimo, 2 interfaces de rede 100Gbps QSFP+;

1.1.8.2.9. Capacidade para suportar, pelo menos, 20 contextos virtuais;

1.1.8.2.10. Possuir fonte de alimentação redundante e hot-swappable;

1.1.8.2.11. Possuir 1 (uma) interface de rede dedicada ao gerenciamento;

1.1.8.2.12. Possuir 1 (uma) interface de rede dedicada para sincronismo;

1.1.8.2.13. Possuir 1 (uma) interface do tipo console ou similar;

1.1.8.2.14. Possuir interface dedicada e física para gerenciamento do equipamento fora de banda. Essa interface deve ser um canal de gerenciamento que funcione mesmo quando o dispositivo é desligado ou não responde. Caso o equipamento não possua essa interface tisica/dedicada, deverá ser composta com outro equipa mento de terceiro onde faça essa função. Não sendo permitido qualquer tipo de configuração de instâncias via software.

1.1.8.2.15. A solução deve possuir mecanismo para dedicar processamento no equipamento de segurança para funções e ações de gerenciamento, mesmo que o equipamento esteja com alto processamento de CPU. Assim evitando a falta de acesso do administrador para qualquer mitigação de problema e aplicação de política para solução de problema. Entre as funções, deve suportar no mínimo: acesso SSH, acesso WEB, alterações de política, comunicação SNMP.

1.1.8.2.16. O Throughput e as interfaces solicitados neste item deverão ser comprovados através de datasheet público na internet. Não serão aceitas declarações de fabricantes informando números de performance e interfaces;

1.1.8.3. FUNCIONALIDADE DE FIREWALL

1.1.8.3.1. A solução deve consistir de appliance de proteção de rede com funcionalidades de proteção de próxima geração;

1.1.8.3.2. 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 técnica;

1.1.8.3.3. O hardware e software que executem as funcionalidades de proteção de rede deve ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

1.1.8.3.4. Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19", incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;

1.1.8.3.5. Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:

1.1.8.3.6. Suporte a, no mínimo, 1024 VLAN Tags 802.1q, agregação de links 802.3ad, policy based routing ou policy based forwarding, roteamento multicast (PIM-SM), DHCP Relay, DHCP Server e Jumbo Frames;

1.1.8.3.7. A solução deve possuir mecanismo onde identifica o volume de conexões que foi trafegada na regra, assim identificando as regras mais utilizadas;

1.1.8.3.8. Deve suportar os seguintes tipos de NAT:

1.1.8.3.9. Nat dinâmico (Many-to-1), Nat estático (1-to-1), Tradução de porta (PAT), NAT de Origem, NAT de Destino e suportar NAT de Origem e NAT de Destino simultaneamente;

1.1.8.3.10. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;

1.1.8.3.11. Deve suportar NAT64 e NAT46;

1.1.8.3.12. Enviar logs para sistemas de monitoração externos, simultaneamente;

1.1.8.3.13. Prover mecanismo contra ataques de falsificação de endereços (IP Spoofing), através da especificação da interface de rede pela qual uma comunicação deve se originar baseado na topologia. Não sendo aceito soluções que utilizem tabela de roteamento para esta proteção;

1.1.8.3.14. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);

1.1.8.3.15. O firewall deve ter a capacidade de operar de forma simultânea em uma única instancia de Firewall, mediante o uso das suas interfaces físicas nos seguintes modos:

transparente, modo sniffer (monitora mento e análise o tráfego de rede), camada 2 (L2) e camada 3 (L3);

1.1.8.3.16. Para IPv6, deve suportar roteamento estático e dinâmico (OSPF);

1.1.8.3.17. Suportar OSPF graceful restart;

1.1.8.3.18. Autenticação integrada via Kerberos.

1.1.8.3.19. Cada regra deve, obrigatoriamente, funcionar nas versões de endereço IP 4 e 6 sem duplicação da base de objetos e regras;

1.1.8.3.20. Não serão aceitas soluções nas quais as interfaces de origem e destino tenham que ser obrigatoriamente explicitadas ou obrigatoriamente listadas nas configurações de regras;

1.1.8.4. FUNCIONALIDADE DE CONTROLE DE DADOS E FILTRO DE CONTEÚDO WEB

1.1.8.4.1. A solução deverá contar com ferramentas de visibilidade e controle de aplicações WEB e Filtro URL integrada no próprio appliance de segurança que permite a criação de políticas de liberação ou bloqueio baseando-se em aplicações WEB e URL;

1.1.8.4.2. Controle de políticas por usuários, grupos de usuários, IPs e redes;

1.1.8.4.3. Deve decriptografar tráfego de entrada e saída em conexões negociadas com TLS 1.2;

1.1.8.4.4. Será aceito soluções de outros fabricantes diferentes do firewall ofertado pela licitante desde que atendido todos os requisitos desta especificação;

1.1.8.4.5. Suportar a atribuição de agendamento às políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

1.1.8.4.6. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:

1.1.8.4.7. Deve ser possível a liberação e bloqueio de aplicações sem a necessidade de liberação de portas e protocolos;

1.1.8.4.8. Reconhecer pelo menos 3.000 (Três mil) aplicações diferentes, incluindo, mas não limitado: a trá fego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

1.1.8.4.9. Para tráfego criptografado (SSL), deve de-criptografar pacotes a fim de possibilitar a leitura do pay load para checagem de assinaturas de aplicações conhecidas;

1.1.8.4.10. A solução deve suportar a recategorização de URLs local;

1.1.8.4.11. Atualizar a base de assinaturas de aplicações automaticamente;

1.1.8.4.12. A solução deve permitir a solicitação da contratada com o fabricante para categorização de URL na base do fabricante;

1.1.8.4.13. Limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e gru pos do LDAP/AD;

1.1.8.4.14. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários;

1.1.8.4.15. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos ou análise heurística;

1.1.8.4.16. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão;

1.1.8.4.17. A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:

1.1.8.4.18. Permitir especificar política por tempo, com definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

1.1.8.4.19. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes;

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

1.1.8.4.21. Deve bloquear o acesso a sites com conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, mesmo que a opção "Safe Search" esteja desabilitada no navegador do usuário;

1.1.8.4.22. Suportar base ou cache de URLs local no appliance, evitando atrasos de comunicação e validação das URLs. Caso a solução ofertada não suporte localmente, será aceito produto externo desde que não seja solução de software livre;

1.1.8.4.23. Suportar a criação de categorias de URLs customizadas; Permitir a customização de página de bloqueio;

1.1.8.4.24. Como melhor prática do uso do acesso a internet e respeitando as políticas de segurança do orgão, a ferramenta deve criar uma página customizada ou pop-up onde o usuário será questionado ou informado no momento do acesso a uma página URL ou applicação WEB de acordo com as políticas de acesso estabelecidas pela area de TI;

1.1.8.4.25. Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via Radius, para a identificação de endereços IP e usuários;

1.1.8.4.26. 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);

1.1.8.4.27. A solução de controle de dados deve trazer de fábrica vários tipos de arquivos reconhecidos nativamente, permitindo a reconhecimento de pelo menos os seguintes tipos de dados e arquivos:

1.1.8.4.27.1. PCI números de cartão de crédito;

1.1.8.4.27.2. Arquivos PDF;

1.1.8.4.27.3. Arquivos executáveis;

1.1.8.4.27.4. Arquivos de banco de dados;

1.1.8.4.27.5. Arquivos do tipo documento;

1.1.8.4.27.6. Arquivos do tipo apresentação;

1.1.8.4.27.7. Arquivos do tipo planilha;

1.1.8.4.28. A solução de controle de dados deve permitir que as direções do tráfego inspecionado sejam defini das no momento da criação da política, tais como: "Upload", "Download" e "Download e Upload".

1.1.8.4.29. A solução de controle de dados deve permitir que o usuário receba uma notificação, redirect de uma página web, sempre que um arquivo reconhecido por match em uma regra em uma das categorias acima, seja feito.

1.1.8.4.30. A solução de controle de dados deve permitir, inspecionar e prevenir vazamentos de arquivos mesmo quando estes sendo trafegados pela Web em páginas utilizando o protocolo HTTPS.

1.1.8.5. FUNCIONALIDADES DE PREVENÇÃO DE AMEAÇAS

1.1.8.5.1. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS e suportar os módulos de: Antivírus e Anti-Malware integrados no próprio equipamento de firewall;

1.1.8.5.2. Possuir capacidade de detecção de, no mínimo, 7.000 (sete mil) assinaturas de ataques pré-definidos;

1.1.8.5.3. A solução deve sincronizar ou aplicar as assinaturas de IPS, Antivírus, Anti- Malware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;

1.1.8.5.4. A fim de não criar indisponibilidade no appliance de segurança, a solução de IPS deve possuir mecanismo de failopen baseado em software, configurável baseado em thresholds de CPU e memória do dispositivo;

1.1.8.5.5. Deve suportar granularidade nas políticas de 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;

1.1.8.5.6. A solução de IPS deve possuir análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, remontagem de pacotes de TCP e bloqueio de pacotes malformados;

1.1.8.5.7. Detectar e bloquear a origem de portscans;

1.1.8.5.8. Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações;

1.1.8.5.9. A solução de IPS, deve suportar a inclusão de novas assinaturas e customização no formato SNORT;

1.1.8.5.10. Possuir assinaturas para bloqueio de ataques de buffer overflow;

1.1.8.5.11. Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP;

1.1.8.5.12. Suportar bloqueio de arquivos por tipo;

1.1.8.5.13. Identificar e bloquear comunicação com botnets;

1.1.8.5.14. Deve suportar referência cruzada com CVE;

1.1.8.5.15. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:

1.1.8.5.16. O nome da assinatura e do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo de proteção;

1.1.8.5.17. Deve suportar a captura de pacotes (PCAP), em assinatura de IPS e Anti-Malware, através da console de gerência centralizada;

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

1.1.8.5.19. Deve suportar a inspeção em arquivos comprimidos (zip, gzip,etc.);

1.1.8.5.20. Possuir a capacidade de prevenção de ameaças não conhecidas;

1.1.8.5.21. Suportar a criação de políticas por Geo Localização, permitindo que o tráfego de determinado País/ Países seja bloqueado;

1.1.8.5.22. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

1.1.8.5.23. A solução de anti-malware, deve ser capaz de detectar e bloquear ações de callbacks;

1.1.8.6. FUNCIONALIDADES DE CONTROLE DE QUALIDADE DE SERVIÇO

1.1.8.6.1. Suportar a criação de políticas de QoS por:

1.1.8.6.2. Endereço de origem, endereço de destino e por porta;

1.1.8.6.3. O QoS deve possibilitar a definição de classes por:

1.1.8.6.3.1. Banda garantida;

1.1.8.6.3.2. Banda máxima ;

1.1.8.6.3.3. Fila de prioridade;

1.1.8.6.3.4. Disponibilizar estatísticas RealTime para classes de QoS;

1.1.8.7. FUNCIONALIDADES DE VPN

1.1.8.7.1. Suportar VPN Site-to-Site e Cliente-To-Site;

1.1.8.7.2. Suportar IPSec VPN;

1.1.8.7.3. Suportar SSL VPN;

1.1.8.7.4. A VPN IPSEc deve suportar:

1.1.8.7.4.1. 3DES, Autenticação MOS e SHA-1, Diffie-Hellman Group 1, Group 2, Group 5 e Group 14, Algorit mo Internet Key Exchange (IKE), AES 128 e 256 (Advanced Encryption Standard) e Autenticação via certificado IKE PKI;

1.1.8.7.5. A solução deve suportar CA Interna e CA Externa de terceiros;

1.1.8.7.6. Solução deve suportar a configuração VPN através de uma interface do tipo GUI (console do fabricante ou interface web);

1.1.8.8. SOLUÇÃO DE PROTEÇÃO CONTRA AMEAÇAS AVANÇADAS

1.1.8.8.1. A solução deverá prover as funcionalidades de inspeção de artefatos de entrada com malwares não conhecidos ou do tipo APT com filtro de ameaças avançadas e análise de execução em tempo real, sendo essa analise executada na nuvem proprietária da próprio fabricante ou appliance dedicada para sandboxing;

1.1.8.8.2. Prevenir através do bloqueio efetivo do malware desconhecido (Dia Zero), oriundo da comunica ção Web (HTTP e HTTPS) e E-mail (SMTP/TLS) via MTA durante análise completa do arquivo no ambiente sandbox, sem que o mesmo seja entregue parcialmente ao cliente.

1.1.8.8.3. A solução deve ser capaz de inspecionar e prevenir malware desconhecido em tráfego criptografado SSL;

1.1.8.8.4. A solução deve fornecer a capacidade de emular ataques em diferentes sistemas operacionais, dentre eles: Windows 7, Windows 8.1 e Windows 10, assim como Office 2003, 2010, 2013 e 2016;

1.1.8.8.5. Implementar atualização da base de dados de forma automática, permitindo agendamentos diários, dias da semana ou dias do mês assim como o período de cada atualização;

1.1.8.8.6. A solução deve suportar as seguintes topologias de implantação: Inline, Message Transfer Agent

1.1.8.8.7. (MTA) e Mirror/TAP;

1.1.8.8.8. A tecnologia de máquina virtual deverá possuir diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso, não sendo baseado apenas em assinaturas;

1.1.8.8.9. A solução de prevença de ameaças avançadas (Sandboxing) contra ataques

persistentes e ZeroDay, deve ser habilitada e funcionar de forma independente, ou seja, não sendo obrigatório o uso e ativação de funcionalidades ou engines de anti-virus para a mesma ter o seu devido funcionamento.

1.1.8.8.10. Todas as máquinas virtuais (Windows e pacote Office) utilizadas na solução e solicitadas neste edital, devem estar integralmente instaladas e licenciadas, sem a necessidade de intervenções por parte do administrador do sistema. As atualizações deverão ser providas pelo fabricante;

1.1.8.8.11. Para a emulação de arquivos, a solução deve suportar arquivos com tamanho máximo de emulação de até 30Mb.

1.1.8.8.12. Implementar mecanismo de exceção, permitindo a criação de regras por VLAN, subrede e endereço IP;

1.1.8.8.13. Implementar a emulação, detecção e bloqueio de qualquer malware e/ou código malicioso detecta do como desconhecido. A solução deve permitir a análise e bloqueio dos seguintes tipos de arquivos caso tenham malware desconhecido: pdf, tar, zip, rar, 7z, exe, rtf, csv, ser, xls, xlsx, xlt, xlm, xltx, xlsm, xltm, xlsb, xla, xlam, xll, xlw, ppt, pptx, pps, pptm, potx, potm, ppam, ppsx, ppsm, doe, docx, dot, doem, dotx, dotm;

1.1.8.8.14. A solução deve permitir a criação de Whitelists baseado no MD5 do arquivo;

1.1.8.8.15. Para melhor administração da solução, a solução deve possibilitar as seguintes

visualizações a nível de monitoração:

1.1.8.8.15.1. Quantidade de arquivos que estão em emulação;

1.1.8.8.15.2. Número de arquivos emulados;

1.1.8.8.15.3. A solução deve possuir os indicadores abaixo referente ao último dia, última semana ou últimos 30 dias:

1.1.8.8.15.3.1. Arquivos scaneados;

1.1.8.8.15.3.2. Arquivos maliciosos;

1.1.9. ITEM 9 NEXT GENERATION FIREWALL DATA CENTER TIPO II

1.1.9.1. CARACTERÍSTICAS GERAIS

1.1.9.1.1. É permitido a composição da solução ofertada entre diversos fabricantes, desde que não contemple solução de software livre;

1.1.9.1.2. A solução deverá ser compatível com SNMPv2 e SNMPv3;

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

1.1.9.1.4. A comunicação entre os appliances de segurança e o módulo de gerência deve ser através de meio criptografado;

1.1.9.1.5. Os appliances de segurança devem suportar operar em cluster ativo-ativo e ativo-passivo sem a necessidade de licenças adicionais;

1.1.9.1.6. Não serão aceitos modelos em listas de end-of-sale, cuja data do fim de vendas seja anterior à data da proposta.

1.1.9.1.7. Não serão aceitos modelos em lista de end-of-support, cuja data do fim do suporte seja anterior ao fim da vigência do contrato e/ou do fim do período de garantia e suporte exigido no edital.

1.1.9.2. CAPACIDADE E QUANTIDADES

1.1.9.2.1. Throughput de, no mínimo, 27.9 Gbps, com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação, anti-malware e prevenção de ameaças avançadas (dia zero) habilitados simultaneamente;

1.1.9.2.2. Suporte a, no mínimo, 18.000.000 (dezoito milhões) de conexões ou sessões simultâneas

1.1.9.2.3. Suporte a, no mínimo, 730.000 (setecentas e trinta mil) novas conexões ou sessões por segundo

1.1.9.2.4. Throughput de, no mínimo, 68 Gbps (sessenta e oito), para conexões VPN;

1.1.9.2.5. Armazenamento redundante de, no mínimo, 900GB SSD;

1.1.9.2.6. Possuir, no mínimo, 4 (quatro) interfaces de rede 25 Gbps SFP28;

1.1.9.2.7. Possuir, no mínimo, 8 (oito) interfaces de rede 10 Gbps SFP+;

1.1.9.2.8. Suportar expansão futura para, no mínimo, 2 interfaces de rede 100/40Gbps QSFP28;

1.1.9.2.9. Capacidade para suportar até 50 contextos virtuais;

1.1.9.2.11. Possuir fonte de alimentação redundante e hot-swappable;

1.1.9.2.12. Possuir 1 (uma) interface de rede dedicada ao gerenciamento;

1.1.9.2.13. Possuir 1 (uma) interface de rede dedicada para sincronismo;

1.1.9.2.14. Possuir 1 (uma) interface do tipo console ou similar;

1.1.9.2.15. Possuir interface dedicada e física para gerenciamento do equipamento fora de banda. Essa interface deve ser um canal de gerenciamento que funcione mesmo quando o dispositivo é desligado ou não responde. Caso o equipamento não possua essa interface tisica/dedicada, deverá ser composta com outro equipamento de terceiro onde faça essa função. Não sendo permitido qualquer tipo de configuração de instancias via software.

1.1.9.2.16. A solução deve possuir mecanismo para dedicar processamento no equipamento de segurança para funções e ações de gerenciamento, mesmo que o equipamento esteja com alto processamento de CPU. Assim evitando a falta de acesso do administrador para qualquer mitigação de problema e aplicação de política para solução de problema. Entre as funções, deve suportar no mínimo: acesso SSH, acesso WEB, alterações de política, comunicação SNMP.

1.1.9.2.17. O Throughput e as interfaces solicitados neste item deverão ser comprovados através de datasheet público na internet. Não serão aceitas declarações de fabricantes informando números de performance e interfaces;

1.1.9.3. FUNCIONALIDADE DE FIREWALL

1.1.9.3.1. A solução deve consistir de appliance de proteção de rede com funcionalidades de proteção de próxima geração;

1.1.9.3.2. 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 técnica;

1.1.9.3.3. O hardware e software que executem as funcionalidades de proteção de rede deve ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

1.1.9.3.4. Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19", incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;

1.1.9.3.5. Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:

1.1.9.3.6. Suporte a, no mínimo, 1024 VLAN Tags 802.1q, agregação de links 802.3ad, policy

based routing ou policy based forwarding, roteamento multicast (PIM-SM), DHCP Relay, DHCP Server e Jumbo Frames;

1.1.9.3.7. A solução deve possuir mecanismo onde identifica o volume de conexões que foi trafegada na regra, assim identificando as regras mais utilizadas;

1.1.9.3.8. Deve suportar os seguintes tipos de NAT:

1.1.9.3.9. Nat dinâmico (Many-to-1), Nat estático (1-to-1), Tradução de porta (PAT), NAT de Origem, NAT de Destino e suportar NAT de Origem e NAT de Destino simultaneamente;

1.1.9.3.10. 4.9.3.10. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;

1.1.9.3.11. Deve suportar NAT64 e NAT46;

1.1.9.3.12. Enviar logs para sistemas de monitoração externos, simultaneamente;

1.1.9.3.13. Prover mecanismo contra ataques de falsificação de endereços (IP Spoofing), através da especificação da interface de rede pela qual uma comunicação deve se originar baseado na topologia. Não sendo acei to soluções que utilizem tabela de roteamento para esta proteção;

1.1.9.3.14. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
1.1.9.3.15. O firewall deve ter a capacidade de operar de forma simultânea em uma única instancia de Firewall, mediante o uso das suas interfaces físicas nos seguintes modos:

transparente, modo sniffer (monitoramento e análise o tráfego de rede), camada 2 (L2) e

camada 3 (L3);

1.1.9.3.16. Para IPv6, deve suportar roteamento estático e dinâmico (OSPF);

1.1.9.3.17. Suportar OSPF graceful restart;

1.1.9.3.18. Autenticação integrada via Kerberos.

1.1.9.3.19. Cada regra deve, obrigatoriamente, funcionar nas versões de endereço IP 4 e 6 sem duplicação da base de objetos e regras;

1.1.9.3.20. Não serão aceitas soluções nas quais as interfaces de origem e destino tenham que ser obrigatoriamente explicitadas ou obrigatoriamente listadas nas configurações de regras;

1.1.9.4. FUNCIONALIDADE DE CONTROLE DE DADOS E FILTRO DE CONTEÚDO WEB

1.1.9.4.1. A solução deverá contar com ferramentas de visibilidade e controle de aplicações WEB e Filtro URL integrada no próprio appliance de segurança que permite a criação de políticas de liberação ou bloqueio baseando-se em aplicações WEB e URL;

1.1.9.4.2. Controle de políticas por usuários, grupos de usuários, IPs e redes;

1.1.9.4.3. Deve decriptografar tráfego de entrada e saída em conexões negociadas com TLS 1.2;

1.1.9.4.4. Será aceito soluções de outros fabricantes diferentes do firewall ofertado pela licitante desde que atendido todos os requisitos desta especificação;

1.1.9.4.5. Suportar a atribuição de agendamento às políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

1.1.9.4.6. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:

1.1.9.4.7. Deve ser possível a liberação e bloqueio de aplicações sem a necessidade de liberação de portas e protocolos;

1.1.9.4.8. Reconhecer pelo menos 3.000 (Três mil) aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de

software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

1.1.9.4.9. Para tráfego criptografado (SSL), deve de-criptografar pacotes a fim de possibilitar a leitura do payload para checagem de assinaturas de aplicações conhecidas;

1.1.9.4.10. A solução deve suportar a recategorização de URLs local;

1.1.9.4.11. Atualizar a base de assinaturas de aplicações automaticamente;

1.1.9.4.12. A solução deve permitir a solicitação da contratada com o fabricante para categorização de URL na base do fabricante;

1.1.9.4.13. Limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD;

1.1.9.4.14. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários;

1.1.9.4.15. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos ou análise heurística;

1.1.9.4.16. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão;

1.1.9.4.17. A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:

1.1.9.4.18. Permitir especificar política por tempo, com definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

1.1.9.4.19. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes;

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

1.1.9.4.21. Deve bloquear o acesso a sites com conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, mesmo que a opção "Safe Search" esteja desabilitada no navegador do usuário;

1.1.9.4.22. Suportar base ou cache de URLs local no appliance, evitando atrasos de comunicação e validação das URLs. Caso a solução ofertada não suporte localmente, será aceito produto externo desde que não seja solução de software livre;

1.1.9.4.23. Suportar a criação de categorias de URLs customizadas;

1.1.9.4.24. Permitir a customização de página de bloqueio;

1.1.9.4.25. Como melhor prática do uso do acesso a internet e respeitando as políticas de segurança do orgão, a ferramenta deve criar uma página customizada ou pop-up onde o usuário será questionado ou informado no momento do acesso a uma página URL ou applicação WEB de acordo com as políticas de acesso estabelecidas pela area de TI;

1.1.9.4.26. Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via Radius, para a identificação de endereços IP e usuários;

1.1.9.4.27. 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);

1.1.9.4.28. A solução de controle de dados deve trazer de fábrica vários tipos de arquivos reconhecidos nativamente, permitindo a reconhecimento de pelo menos os seguintes tipos de

dados e arquivos:

1.1.9.4.28.1. PCI números de cartão de crédito;

1.1.9.4.28.2. Arquivos PDF;

1.1.9.4.28.3. Arquivos executáveis;

1.1.9.4.28.4. Arquivos de banco de dados;

1.1.9.4.28.5. Arquivos do tipo documento;

1.1.9.4.28.6. Arquivos do tipo apresentação;

1.1.9.4.28.7. Arquivos do tipo planilha;

1.1.9.4.29. A solução de controle de dados deve permitir que as direções do tráfego inspecionado sejam defini das no momento da criação da politica, tais como: "Upload", "Download" e "Download e Upload".

1.1.9.4.30. A solução de controle de dados deve permir que o usuário receba uma notificação, redirect de uma página web, sempre que um arquivo reconhecido por match em uma regra em uma das categorias acima, seja feito.

1.1.9.4.31. A solução de controle de dados deve permitir, inspecionar e prevenir vazamentos de arquivos mesmo quando estes estes sendo trafegados pela Web em páginas utilizando o protocolo HTTPS.

1.1.9.5. FUNCIONALIDADES DE PREVENÇÃO DE AMEAÇAS

1.1.9.5.1. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS e suportar os módulos de: Antivírus e Anti-Malware integrados no próprio equipamento de firewall;

1.1.9.5.2. Possuir capacidade de detecção de, no mínimo, 7.000 (sete mil) assinaturas de ataques pré-definidos;

1.1.9.5.3. A solução deve sincronizar ou aplicar as assinaturas de IPS, Antivírus, Anti- Malware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;

1.1.9.5.4. A fim de não criar indisponibilidade no appliance de segurança, a solução de IPS deve possuir me canismo de failopen baseado em software, configurável baseado em thresholds de CPU e memória do disposi tivo;

1.1.9.5.5. Deve suportar granularidade nas políticas de 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;

1.1.9.5.6. A solução de IPS deve possuir análise de padrões de estado de conexões, análise de decodifica ção de protocolo, análise para detecção de anomalias de protocolo, remontagem de pacotes de TCP e bloqueio de pacotes malformados;

1.1.9.5.7. Detectar e bloquear a origem de portscans;

1.1.9.5.8. Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações;

1.1.9.5.9. A solução de IPS, deve suportar a inclusão de novas assinaturas e customização no formato SNORT;

1.1.9.5.10. Possuir assinaturas para bloqueio de ataques de buffer overflow;

1.1.9.5.11. Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP;

1.1.9.5.12. Suportar bloqueio de arquivos por tipo;

1.1.9.5.13. Identificar e bloquear comunicação com botnets;

1.1.9.5.14. Deve suportar referência cruzada com CVE;

1.1.9.5.15. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:

1.1.9.5.16. O nome da assinatura e do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo de proteção;

1.1.9.5.17. Deve suportar a captura de pacotes (PCAP), em assinatura de IPS e Anti-Malware, através da console de gerência centralizada;

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

1.1.9.5.19. Deve suportar a inspeção em arquivos comprimidos (zip, gzip,etc.);

1.1.9.5.20. Possuir a capacidade de prevenção de ameaças não conhecidas;

1.1.9.5.21. Suportar a criação de políticas por Geo Localização, permitindo que o tráfego de determinado País/ Países seja bloqueado;

1.1.9.5.22. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

1.1.9.5.23. A solução de anti-malware, deve ser capaz de detectar e bloquear ações de callbacks;

1.1.9.6. FUNCIONALIDADES DE CONTROLE DE QUALIDADE DE SERVIÇO

1.1.9.6.1. Suportar a criação de políticas de QoS por:

1.1.9.6.2. Endereço de origem, endereço de destino e por porta;

1.1.9.6.3. O QoS deve possibilitar a definição de classes por:

1.1.9.6.4. Banda garantida;

1.1.9.6.5. Banda máxima ;

1.1.9.6.6. Fila de prioridade;

1.1.9.6.7. Disponibilizar estatísticas RealTime para classes de QoS;

1.1.9.7. FUNCIONALIDADES DE VPN

1.1.9.7.1. Suportar VPN Site-to-Site e Cliente-To-Site;

1.1.9.7.2. Suportar IPSec VPN;

1.1.9.7.3. Suportar SSL VPN;

1.1.9.7.4. A VPN IPSEc deve suportar:

1.1.9.7.5. 3DES, Autenticação MOS e SHA-1, Diffie-Hellman Group 1, Group 2, Group 5 e Group 14, Algoritmo Internet Key Exchange (IKE), AES 128 e 256 (Advanced Encryption Standard) e Autenticação via certificado IKE PKI;

1.1.9.7.6. A solução deve suportar CA Interna e CA Externa de terceiros;

1.1.9.7.7. Solução deve suportar a configuração VPN através de uma interface do tipo GUI (console do fabricante ou interface web);

1.1.9.8. SOLUÇÃO DE PROTEÇÃO CONTRA AMEAÇAS AVANÇADAS

1.1.9.8.1. A solução deverá prover as funcionalidades de inspeção de artefatos de entrada com malwares não conhecidos ou do tipo APT com filtro de ameaças avançadas e análise de execução em tempo real, sendo essa analise executada na nuvem proprietária da próprio fabricante ou appliance dedicada para sandboxing;

1.1.9.8.2. Prevenir através do bloqueio efetivo do malware desconhecido (Dia Zero), oriundo da comunica ção Web (HTTP e HTTPS) e E-mail (SMTP/TLS) via MTA durante análise completa do arquivo no ambiente sandbox, sem que o mesmo seja entregue parcialmente ao cliente.

1.1.9.8.3. A solução deve ser capaz de inspecionar e prevenir malware desconhecido em tráfego criptografado SSL;

1.1.9.8.4. A solução deve fornecer a capacidade de emular ataques em diferentes sistemas operacionais, dentre eles: Windows 7, Windows 8.1 e Windows 10, assim como Office 2003, 2010, 2013 e 2016;

1.1.9.8.5. Implementar atualização da base de dados de forma automática, permitindo agendamentos diários, dias da semana ou dias do mês assim como o período de cada atualização;

1.1.9.8.6. A solução deve suportar as seguintes topologias de implantação: Inline, Message Transfer Agent (MTA) e Mirrar/TAP;

1.1.9.8.7. A tecnologia de máquina virtual deverá possuir diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso, não sendo baseado apenas em assinaturas;

1.1.9.8.8. A solução de prevença de ameaças avançadas (Sandboxing) contra ataques persistentes e ZeroDay, deve ser habilitada e funcionar de forma independente, ou seja, não sendo obrigatório o uso e ativação de funcionalidades ou engines de anti-virus para a mesma ter o seu devido funcionamento.

1.1.9.8.9. Todas as máquinas virtuais (Windows e pacote Office) utilizadas na solução e solicitadas neste edital, devem estar integralmente instaladas e licenciadas, sem a necessidade de intervenções por parte do admi nistrador do sistema. As atualizações deverão ser providas pelo fabricante;

1.1.9.8.10. Para a emulação de arquivos, a solução deve suportar arquivos com tamanho máximo de emulação de até 30Mb.

1.1.9.8.11. Implementar mecanismo de exceção, permitindo a criação de regras por VLAN, subrede e endereço IP;

1.1.9.8.12. Implementar a emulação, detecção e bloqueio de qualquer malware e/ou código malicioso detecta do como desconhecido. A solução deve permitir a análise e bloqueio dos seguintes tipos de arquivos caso tenham malware desconhecido: pdf, tar, zip, rar, 7z, exe, rtf, csv, ser, xls, xlsx, xlt, xlm, xltx, xlsm, xltm, xlsb, xla, xlam, xll, xlw, ppt, pptx, pps, pptm, potx, potm, ppam, ppsx, ppsm, doe, docx, dot, doem, dotx, dotm;

1.1.9.8.13. A solução deve permitir a criação de Whitelists baseado no MD5 do arquivo;

1.1.9.8.14. Para melhor administração da solução, a solução deve possibilitar as seguintes

visualizações a nível de monitoração:

1.1.9.8.14.1. Quantidade de arquivos que estão em emulação;

1.1.9.8.14.2. 4.9.8.14.2. Número de arquivos emulados;

1.1.9.8.15. A solução deve possuir os indicadores abaixo referente ao último dia, última semana ou últimos 30 dias:

1.1.9.8.15.1. Arquivos scaneados;

1.1.9.8.15.2. Arquivos maliciosos;

1.1.10. ITEM 10 NEXT GENERATION FIREWALL DATA CENTER TIPO III

1.1.10.1. CARACTERÍSTICAS GERAIS

1.1.10.1.1. É permitido a composição da solução ofertada entre diversos fabricantes, desde que não contemple solução de software livre;

1.1.10.1.2. A solução deverá ser compatível com SNMPv2 e SNMPv3;

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

1.1.10.1.4. A comunicação entre os appliances de segurança e o módulo de gerência deve ser através de meio criptografado;

1.1.10.1.5. Os appliances de segurança devem suportar operar em cluster ativo-ativo e ativo-passivo sem a necessidade de licenças adicionais;

1.1.10.1.6. Não serão aceitos modelos em listas de end-of-sale, cuja data do fim de vendas seja anterior à data da proposta.

1.1.10.1.7. Não serão aceitos modelos em lista de end-of-support, cuja data do fim do suporte seja anterior ao fim da vigência do contrato e/ou do fim do período de garantia e suporte exigido no edital.

1.1.10.2. CAPACIDADE E QUANTIDADES

1.1.10.2.1. Throughput de, no mínimo, 44 Gbps, com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação, anti-malware e prevenção de ameaças avançadas (dia zero) habilitados simultaneamente;

1.1.10.2.2. Suporte a, no mínimo, 42.000.000 (quarenta e duas milhões) de conexões ou sessões simultâneas;

1.1.10.2.3. Suporte a, no mínimo, 1.100.000 (um milhão e cem mil) novas conexões ou sessões por segundo

1.1.10.2.4. Throughput de, no mínimo, 95 Gbps (noventa e cinco), para conexões VPN;

1.1.10.2.5. Armazenamento redundante de, no mínimo, 900GB SSD;

1.1.10.2.6. Possuir, no mínimo, 12 (doze) interfaces de rede 10 Gbps SFP+;

1.1.10.2.7. Possuir, no mínimo, 4 (quatro) interfaces de rede 10/25 Gbps SFP28;

1.1.10.2.9. Suportar expansão futura para, no mínimo, 2 interfaces de rede 100/40Gbps QSFP28

Capacidade para suportar até 75 contextos virtuais;

1.1.10.2.10. Possuir fonte de alimentação redundante;

1.1.10.2.12. Possuir 1 (uma) interface de rede dedicada ao gerenciamento;

1.1.10.2.13. Possuir 1 (uma) interface de rede dedicada para sincronismo;

1.1.10.2.14. Possuir 1 (uma) interface do tipo console ou similar;

1.1.10.2.15. Possuir interface dedicada e física para gerenciamento do equipamento fora de banda. Essa interface deve ser um canal de gerenciamento que funcione mesmo quando o dispositivo é desligado ou não responde. Caso o equipamento não possua essa interface tisica/dedicada, deverá ser composta com outro equipamento de terceiro onde faça essa função. Não sendo permitido qualquer tipo de configuração de instancias via software.

1.1.10.2.16. A solução deve possuir mecanismo para dedicar processamento no equipamento de segurança para funções e ações de gerenciamento, mesmo que o equipamento esteja com alto processamento de CPU. Assim evitando a falta de acesso do administrador para qualquer mitigação de problema e aplicação de política para solução de problema. Entre as funções, deve suportar no mínimo: acesso SSH, acesso WEB, alterações de política, comunicação SNMP.

1.1.10.2.17. O Throughput e as interfaces solicitados neste item deverão ser comprovados através de datasheet público na internet. Não serão aceitas declarações de fabricantes informando números de performance e interfaces;

1.1.10.3. FUNCIONALIDADE DE FIREWALL

1.1.10.3.1. A solução deve consistir de appliance de proteção de rede com funcionalidades de proteção de próxima geração;

1.1.10.3.2. 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 técnica;

1.1.10.3.3. O hardware e software que executem as funcionalidades de proteção de rede deve ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

1.1.10.3.4. Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19", incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;

1.1.10.3.5. Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:

1.1.10.3.6. Suporte a, no mínimo, 1024 VLAN Tags 802.1q, agregação de links 802.3ad, policy based routing ou policy based forwarding, roteamento multicast (PIM-SM), DHCP Relay, DHCP Server e Jumbo Frames;

1.1.10.3.7. A solução deve possuir mecanismo onde identifica o volume de conexões que foi trafegada na regra, assim identificando as regras mais utilizadas;

1.1.10.3.8. Deve suportar os seguintes tipos de NAT:

1.1.10.3.9. Nat dinâmico (Many-to-1), Nat estático (1-to-1), Tradução de porta (PAT), NAT de Origem, NAT de Destino e suportar NAT de Origem e NAT de Destino simultaneamente;

1.1.10.3.10. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;

1.1.10.3.11. Deve suportar NAT64 e NAT46;

1.1.10.3.12. Enviar logs para sistemas de monitoração externos, simultaneamente;

1.1.10.3.13. Prover mecanismo contra ataques de falsificação de endereços (IP Spoofing),

através da especificação da interface de rede pela qual uma comunicação deve se originar

baseado na topologia. Não sendo aceito soluções que utilizem tabela de roteamento para esta proteção;

1.1.10.3.14. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);

1.1.10.3.15. O firewall deve ter a capacidade de operar de forma simultânea em uma única instancia de Firewall, mediante o uso das suas interfaces físicas nos seguintes modos:

transparente, modo sniffer (monitoramento e análise o tráfego de rede), camada 2 (L2) e

camada 3 (L3);

1.1.10.3.16. Para IPv6, deve suportar roteamento estático e dinâmico (OSPF);

1.1.10.3.17. Suportar OSPF graceful restart;

1.1.10.3.18. Autenticação integrada via Kerberos.

1.1.10.3.19. Cada regra deve, obrigatoriamente, funcionar nas versões de endereço IP 4 e 6 sem duplicação da base de objetos e regras;

1.1.10.3.20. Não serão aceitas soluções nas quais as interfaces de origem e destino tenham que

ser obrigatoariamente explicitadas ou obrigatoriamente listadas nas configurações de regras;

1.1.10.4. FUNCIONALIDADE DE CONTROLE DE DADOS E FILTRO DE CONTEÚDO WEB

1.1.10.4.1. A solução deverá contar com ferramentas de visibilidade e controle de aplicações WEB e Filtro URL integrada no próprio appliance de segurança que permite a criação de políticas de liberação ou bloqueio baseando-se em aplicações WEB e URL;

1.1.10.4.2. Controle de políticas por usuários, grupos de usuários, IPs e redes;

1.1.10.4.3. Deve decriptografar tráfego de entrada e saída em conexões negociadas com TLS 1.2;

1.1.10.4.4. Será aceito soluções de outros fabricantes diferentes do firewall ofertado pela licitante desde que atendido todos os requisitos desta especificação;

1.1.10.4.5. Suportar a atribuição de agendamento às políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

1.1.10.4.6. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, inde pendente de porta e protocolo, com as seguintes funcionalidades:

1.1.10.4.7. Deve ser possível a liberação e bloqueio de aplicações sem a necessidade de liberação de portas e protocolos;

1.1.10.4.8. Reconhecer pelo menos 3.000 (Três mil) aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áu dio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

1.1.10.4.9. Para tráfego criptografado (SSL), deve decriptografar pacotes a fim de possibilitar a leitura do pay load para checagem de assinaturas de aplicações conhecidas;

1.1.10.4.10. A solução deve suportar a recategorização de URLs local;

1.1.10.4.11. Atualizar a base de assinaturas de aplicações automaticamente;

1.1.10.4.12. A solução deve permitir a solicitação da contratada com o fabricante para categorização de URL na base do fabricante;

1.1.10.4.13. Limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD;

1.1.10.4.14. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Aclive Directory, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários;

1.1.10.4.15. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos ou análise heurística;

1.1.10.4.16. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão;

1.1.10.4.17. A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:

1.1.10.4.18. Permitir especificar política por tempo, com definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

1.1.10.4.19. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes;

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

1.1.10.4.21. Deve bloquear o acesso a sites com conteúdo indevido ao utilizar a busca em sites

como Google, Bing e Yahoo, mesmo que a opção "Safe Search" esteja desabilitada no navegador do usuário;

1.1.10.4.22. Suportar base ou cache de URLs local no appliance, evitando atrasos de comunicação e validação das URLs. Caso a solução ofertada não suporte localmente, será aceito produto externo desde que não seja solução de software livre;

1.1.10.4.23. Suportar a criação de categorias de URLs customizadas;

1.1.10.4.24. Permitir a customização de página de bloqueio;

1.1.10.4.25. Como melhor prática do uso do acesso a internet e respeitando as políticas de segurança do orgão, a ferramenta deve criar uma página customizada ou pop-up onde o usuário será questionado ou informado no momento do acesso a uma página URL ou applicação WEB de acordo com as políticas de acesso estabelecidas pela area de TI;

1.1.10.4.26. Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via Radius, para a identificação de endereços IP e usuários;

1.1.10.4.27. 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);

1.1.10.4.28. A solução de controle de dados deve trazer de fábrica vários tipos de arquivos reconhecidos nativamente, permitindo a reconhecimento de pelo menos os seguintes tipos de dados e arquivos:

1.1.10.4.28.1. PCI números de cartão de crédito;

1.1.10.4.28.2. Arquivos PDF;

1.1.10.4.28.3. Arquivos executáveis;

1.1.10.4.28.4. Arquivos de banco de dados;

1.1.10.4.28.5. Arquivos do tipo documento;

1.1.10.4.28.6. Arquivos do tipo apresentação;

1.1.10.4.28.7. Arquivos do tipo planilha;

1.1.10.4.29. A solução de controle de dados deve permitir que as direções do tráfego inspecionado sejam definidas no momento da criação da politica, tais como: "Upload", "Download" e "Download e Upload".

1.1.10.4.30. A solução de controle de dados deve permir que o usuário receba uma notificação, redirect de uma página web, sempre que um arquivo reconhecido por match em uma regra em uma das categorias acima, seja feito.

1.1.10.4.31. A solução de controle de dados deve permitir, inspecionar e prevenir vazamentos de arquivos mesmo quando estes estes sendo trafegados pela Web em páginas utilizando o protocolo HTTPS.

1.1.10.5. FUNCIONALIDADES DE PREVENÇÃO DE AMEAÇAS

1.1.10.5.1. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS e suportar os módulos de: Antivírus e Anti-Malware integrados no próprio equipamento de firewall;

1.1.10.5.2. Possuir capacidade de detecção de, no mínimo, 7.000 (sete mil) assinaturas de ataques pré-definidos;

1.1.10.5.3. A solução deve sincronizar ou aplicar as assinaturas de IPS, Antivírus, Anti- Malware quando imple mentado em alta disponibilidade ativo/ativo e ativo/passivo;

1.1.10.5.4. A fim de não criar indisponibilidade no appliance de segurança, a solução de IPS deve possuir mecanismo de fail-open baseado em software, configurável baseado em thresholds de CPU e memória do dispositivo;

1.1.10.5.5. Deve suportar granularidade nas políticas de 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;

1.1.10.5.6. A solução de IPS deve possuir análise de padrões de estado de conexões, análise de decodifica ção de protocolo, análise para detecção de anomalias de protocolo, remontagem de pacotes de TCP e bloqueio de pacotes malformados;

1.1.10.5.7. Detectar e bloquear a origem de portscans;

1.1.10.5.8. Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações;

1.1.10.5.9. A solução de IPS, deve suportar a inclusão de novas assinaturas e customização no formato

1.1.10.5.10. Possuir assinaturas para bloqueio de ataques de buffer overflow;

1.1.10.5.11. Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP; Suportar bloqueio de arquivos por tipo;

1.1.10.5.12. Identificar e bloquear comunicação com botnets; Deve suportar referência cruzada com CVE;

1.1.10.5.13. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:

1.1.10.5.14. O nome da assinatura e do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo de proteção;

1.1.10.5.15. Deve suportar a captura de pacotes (PCAP), em assinatura de IPS e Anti-Malware, através da console de gerência centralizada;

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

1.1.10.5.17. Deve suportar a inspeção em arquivos comprimidos (zip, gzip,etc.);

1.1.10.5.18. Possuir a capacidade de prevenção de ameaças não conhecidas;

1.1.10.5.19. Suportar a criação de políticas por Geo Localização, permitindo que o tráfego de determinado País/ Países seja bloqueado;

1.1.10.5.20. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

1.1.10.5.21. A solução de anti-malware, deve ser capaz de detectar e bloquear ações de callbacks;

1.1.10.6. FUNCIONALIDADES DE CONTROLE DE QUALIDADE DE SERVIÇO

1.1.10.6.1. Suportar a criação de políticas de QoS por:

1.1.10.6.2. Endereço de origem, endereço de destino e por porta;

1.1.10.6.3. O QoS deve possibilitar a definição de classes por:

1.1.10.6.4. Banda garantida;

1.10.6.3.2. Banda máxima ;

1.10.6.3.3. Fila de prioridade;

1.1.10.6.5. Disponibilizar estatísticas RealTime para classes de QoS;

1.1.**10.7. FUNCIONALIDADES DE VPN**

1.1.10.7.1. Suportar VPN Site-to-Site e Cliente-To-Site;

1.1.10.7.2. Suportar IPSec VPN;

1.1.10.7.3. Suportar SSL VPN;

1.1.10.7.4. A VPN IPSEc deve suportar:

1.1.10.7.5. 3DES, Autenticação MOS e SHA-1, Diffie-Hellman Group 1, Group 2, Group 5 e Group 14, Algorit mo Internet Key Exchange (IKE), AES 128 e 256 (Advanced Encryption Standard) e Autenticação via certificado IKE PKI;

1.1.10.7.6. A solução deve suportar CA Interna e CA Externa de terceiros;

1.1.10.7.7. Solução deve suportar a configuração VPN através de uma interface do tipo GUI (console do fabricante ou interface web);

1.1.10.8. SOLUÇÃO DE PROTEÇÃO CONTRA AMEAÇAS AVANÇADAS

1.1.10.8.1. A solução deverá prover as funcionalidades de inspeção de artefatos de entrada com malwares não conhecidos ou do tipo APT com filtro de ameaças avançadas e análise de execução em tempo real, sendo essa analise executada na nuvem proprietária do próprio fabricante ou appliance dedicada para sandboxing;

1.1.10.8.2. Prevenir através do bloqueio efetivo do malware desconhecido (Dia Zero), oriundo da comunicação Web (HTTP e HTTPS) e E-mail (SMTP/TLS) via MTA durante análise completa do arquivo no ambiente sandbox, sem que o mesmo seja entregue parcialmente ao cliente.

1.1.10.8.3. A solução deve ser capaz de inspecionar e prevenir malware desconhecido em tráfego criptografado SSL;

1.1.10.8.4. A solução deve fornecer a capacidade de emular ataques em diferentes sistemas operacionais, dentre eles: Windows 7, Windows 8.1 e Windows 10, assim como Office 2003, 2010, 2013 e 20 16;

1.1.10.8.5. Implementar atualização da base de dados de forma automática, permitindo agendamentos diários, dias da semana ou dias do mês assim como o período de cada atualização;

1.1.10.8.6. A solução deve suportar as seguintes topologias de implantação: Inline, Message Transfer Agent (MTA) e Mirror/TAP;

1.1.10.8.7. A tecnologia de máquina virtual deverá possuir diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso, não sendo baseado apenas em assinaturas;

1.1.10.8.8. A solução de prevença de ameaças avançadas (Sandboxing) contra ataques persistentes e ZeroDay, deve ser habilitada e funcionar de forma independente, ou seja, não sendo obrigatório o uso e ativação de funcionalidades ou engines de anti-virus para a mesma ter o seu devido funcionamento.

1.1.10.8.9. Todas as máquinas virtuais (Windows e pacote Office) utilizadas na solução e solicitadas neste edital, devem estar integralmente instaladas e licenciadas, sem a necessidade de intervenções por parte do administrador do sistema. As atualizações deverão ser providas pelo fabricante;

1.1.10.8.10. 4.10.8.10. Para a emulação de arquivos, a solução deve suportar arquivos com tamanho máximo de emulação de até 30Mb.

1.1.10.8.11. Implementar mecanismo de exceção, permitindo a criação de regras por VLAN, subrede e endere ço IP;

1.1.10.8.12. Implementar a emulação, detecção e bloqueio de qualquer malware e/ou código malicioso detecta do como desconhecido. A solução deve permitir a análise e bloqueio dos seguintes tipos de arquivos caso te nham malware desconhecido: pdf, tar, zip, rar, 7z, exe, rtf, csv, ser, xls, xlsx, xlt, xlm, xltx, xlsm, xltm, xlsb, xla, xlam, xll, xlw, ppt, pptx, pps, pptm, potx, potm, ppam, ppsx, ppsm, doe, docx, dot, doem, dotx, dotm;

1.1.10.8.13. A solução deve permitir a criação de Whitelists baseado no MD5 do arquivo;
1.1.10.8.14. Para melhor administração da solução, a solução deve possibilitar as seguintes

visualizações a nível de monitoração:

1.1.10.8.14.1. Quantidade de arquivos que estão em emulação;

1.10.8.14.2. Número de arquivos emulados;

1.1.10.8.14.2. A solução deve possuir os indicadores abaixo referente ao último dia, última semana ou últimos 30 dias:

1.1.10.8.14.3. Arquivos scaneados;

1.1.10.8.14.4. Arquivos maliciosos;

1.1.11. ITEM 11 - NEXT GENERATION FIREWALL PARA NUVEM PRIVADA

1.1.11.1. CARACTERÍSTICAS GERAIS

1.1.11.1.1. O licenciamento deverá ser feito pelo número de cores virtuais;

1.1.11.1.2. Deve ser compatível com, pelo menos, os seguintes hypervisors: VMware ESXi, Microsoft Hyper-V e KVM;

1.1.11.1.3. A solução deverá permitir expansão através de adição de novas licenças, de forma que suporte a criação de "pools" de gateways virtuais;

1.1.11.1.4. A solução para ambientes virtualizados deve suportar os seguintes SDN de mercado para integração, como: OpenStack, Cisco ACI, VMware NSX, e ESXi.

1.1.11.2. FUNCIONALIDADE DE FIREWALL

1.1.11.2.1. A solução deve consistir de appliance de proteção de rede com funcionalidades de proteção de próxima geração;

1.1.11.2.2. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplas instâncias desde que obedeçam a todos os requisitos desta especificação técnica;

1.1.11.2.3. Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:

1.1.11.2.4. Suporte a, no mínimo, 1024 VLAN Tags 802.1q, agregação de links 802.3ad, policy based routing ou policy based forwarding, roteamento multicast (PIM-SM), DHCP Relay, DHCP Server e Jumbo Frames;

1.1.11.2.5.

1.1.11.2.6. A solução deve possuir mecanismo onde identifica o volume de conexões que foi trafegada na regra, assim identificando as regras mais utilizadas;

1.1.11.2.7. Deve suportar os seguintes tipos de NAT:

1.1.11.2.8. Nat dinâmico (Many-to-1), Nat estático (1-to-1), Tradução de porta (PAT), NAT de Origem, NAT de Destino e suportar NAT de Origem e NAT de Destino simultaneamente;

1.1.11.2.9. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de rotea mento assimétrico;

1.1.11.2.10. Deve suportar NAT64 e NAT46;

1.1.11.2.11. Enviar logs para sistemas de monitoração externos, simultaneamente;

1.1.11.2.12. Prover mecanismo contra ataques de falsificação de endereços (IP Spoofing), através da especificação da interface de rede pela qual uma comunicação deve se originar baseado na topologia. Não sendo aceito soluções que utilizem tabela de roteamento para esta proteção;

1.1.11.2.13. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);

1.1.11.2.14. O firewall deve ter a capacidade de operar de forma simultânea em uma única instancia de Firewall, mediante o uso das suas interfaces físicas nos seguintes modos: transparente, modo sniffer (monitoramento e análise o tráfego de rede), camada 2 (L2) e camada 3 (L3);

1.1.11.2.15. Para IPv6, deve suportar roteamento estático e dinâmico (OSPF);

1.1.11.2.16. Suportar OSPF graceful restart;

1.1.11.2.17. Autenticação integrada via Kerberos.

1.1.11.2.18. Cada regra deve, obrigatoriamente, funcionar nas versões de endereço IP 4 e 6 sem duplicação da base de objetos e regras;

1.1.11.2.19. Não serão aceitas soluções nas quais as interfaces de origem e destino tenham que ser obrigatoriamente explicitadas ou obrigatoriamente listadas nas configurações de regras;

1.1.11.3. FUNCIONALIDADE DE CONTROLE DE DADOS E FILTRO DE CONTEÚDO WEB

1.1.11.3.1. A solução deverá contar com ferramentas de visibilidade e controle de aplicações WEB e Filtro URL integrada no próprio appliance de segurança que permite a criação de políticas de liberação ou bloqueio baseando-se em aplicações WEB e URL;

1.1.11.3.2. Controle de políticas por usuários, grupos de usuários, IPs e redes;

1.1.11.3.3. Deve de-criptografar tráfego de entrada e saída em conexões negociadas com TLS 1.2;

1.1.11.3.4. Será aceito soluções de outros fabricantes diferentes do firewall ofertado pela licitante desde que atendido todos os requisitos desta especificação;

1.1.11.3.5. Suportar a atribuição de agendamento às políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

1.1.11.3.6. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, inde pendente de porta e protocolo, com as seguintes funcionalidades:

1.1.11.3.7. Deve ser possível a liberação e bloqueio de aplicações sem a necessidade de liberação de portas e protocolos;

1.1.11.3.8. Reconhecer pelo menos 3.000 (Três mil) aplicações diferentes, incluindo, mas não limitado: a tráfe go relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áu dio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

1.1.11.3.9. Para tráfego criptografado (SSL), deve decriptografar pacotes a fim de possibilitar a leitura do pay load para checagem de assinaturas de aplicações conhecidas;

1.1.11.3.10. A solução deve suportar a recategorização de URLs local;

1.1.11.3.11. Atualizar a base de assinaturas de aplicações automaticamente;

1.1.11.3.12. A solução deve permitir a solicitação da contratada com o fabricante para categorização de URL na base do fabricante;

1.1.11.3.13. Limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD;

1.1.11.3.14. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários;

1.1.11.3.15. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos ou análise heurística;

1.1.11.3.16. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão;

1.1.11.3.17. A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:

1.1.11.3.18. Permitir especificar política por tempo, com definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

1.1.11.3.19. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes;

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

1.1.11.3.21. Deve bloquear o acesso a sites com conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, mesmo que a opção "Safe Search" esteja desabilitada no navegador do usuário;

1.1.11.3.22. Suportar base ou cache de URLs local no appliance, evitando atrasos de comunicação e validação das URLs. Caso a solução ofertada não suporte localmente, será aceito produto externo desde que não seja solução de software livre;

1.1.11.3.23. Suportar a criação de categorias de URLs customizadas;

1.1.11.3.24. Permitir a customização de página de bloqueio;

1.1.11.3.25. Como melhor prática do uso do acesso a internet e respeitando as políticas de segurança do orgão, a ferramenta deve criar uma página customizada ou pop-up onde o usuário será questionado ou informado no momento do acesso a uma página URL ou applicação WEB de acordo com as políticas de acesso estabelecidas pela area de TI;

1.1.11.3.26. Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via Radius, para a identificação de endereços IP e usuários;

1.1.11.3.27. 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);

1.1.11.3.28. A solução de controle de dados deve trazer de fábrica vários tipos de arquivos reconhecidos nativamente, permitindo a reconhecimento de pelo menos os seguintes tipos de dados e arquivos:

1.1.11.3.28.1. PCI números de cartão de crédito;

1.1.11.3.28.2. Arquivos PDF;

1.1.11.3.28.3. Arquivos executáveis;

1.1.11.3.28.4. Arquivos de banco de dados;

1.1.11.3.28.5. Arquivos do tipo documento;

1.1.11.3.28.6. Arquivos do tipo apresentação;

1.1.11.3.28.7. Arquivos do tipo planilha;

1.1.11.3.29. A solução de controle de dados deve permitir que as direções do tráfego inspecionado sejam definidas no momento da criação da política, tais como: "Upload", "Download" e "Download e Upload".

1.1.11.3.30. A solução de controle de dados deve permir que o usuário receba uma notificação, redirect de uma página web, sempre que um arquivo reconhecido por match em uma regra em uma das categorias acima, seja feito.

1.1.11.3.31. A solução de controle de dados deve permitir, inspecionar e prevenir vazamentos de arquivos mes mo quando estes estes sendo trafegados pela Web em páginas utilizando o protocolo HTTPS.

1.1.11.4. FUNCIONALIDADES DE PREVENÇÃO DE AMEAÇAS

1.1.11.4.1. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS e suportar os módulos de: Antivírus e Anti-Malware integrados no próprio equipamento de firewall;

1.1.11.4.2. Possuir capacidade de detecção de, no mínimo, 7.000 (sete mil) assinaturas de ataques pré-definidos;

1.1.11.4.3. A solução deve sincronizar ou aplicar as assinaturas de IPS, Antivírus, Anti- Malware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;

1.1.11.4.4. A fim de não criar indisponibilidade no appliance de segurança, a solução de IPS deve possuir me canismo de fail-open baseado em software, configurável baseado em thresholds de CPU e memória do dispositivo;

1.1.11.4.5. Deve suportar granularidade nas políticas de 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;

1.1.11.4.6. A solução de IPS deve possuir análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, remontagem de pacotes de TCP e bloqueio de pacotes malformados;

1.1.11.4.7. Detectar e bloquear a origem de portscans;

1.1.11.4.8. Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinatu ras e customizações;

1.1.11.4.9. A solução de IPS, deve suportar a inclusão de novas assinaturas e customização no formato SNORT;

1.1.11.4.10. Possuir assinaturas para bloqueio de ataques de buffer overflow;

1.1.11.4.11. Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP;

1.1.11.4.12. Suportar bloqueio de arquivos por tipo;

1.1.11.4.13. Identificar e bloquear comunicação com botnets;

1.1.11.4.14. Deve suportar referência cruzada com CVE;

1.1.11.4.15. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:

1.1.11.4.16. O nome da assinatura e do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo de proteção;

1.1.11.4.17. Deve suportar a captura de pacotes (PCAP), em assinatura de IPS e Anti-Malware, através da con sole de gerência centralizada;

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

1.1.11.4.19. Deve suportar a inspeção em arquivos comprimidos (zip, gzip,etc.);

1.1.11.4.20. Possuir a capacidade de prevenção de ameaças não conhecidas;

1.1.11.4.21. Suportar a criação de políticas por Geo Localização, permitindo que o tráfego de determinado País/ Países seja bloqueado;

1.1.11.4.22. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

1.1.11.4.23. A solução de anti-malware, deve ser capaz de detectar e bloquear ações de callbacks;

1.1.11.5. FUNCIONALIDADES DE CONTROLE DE QUALIDADE DE SERVIÇO

1.1.11.5.1. Suportar a criação de políticas de QoS por:

1.1.11.5.2. Endereço de origem, endereço de destino e por porta;

1.1.11.5.3. O QoS deve possibilitar a definição de classes por:

1.1.11.5.4. Banda garantida; 4.11.5.3.2. Banda máxima; 4.11.5.3.3. Fila de prioridade;
1.1.11.5.5. Disponibilizar estatísticas RealTime para classes de QoS;

1.1.11.6. FUNCIONALIDADES DE VPN

1.1.11.6.1. Suportar VPN Site-to-Site e Cliente-To-Site;

1.1.11.6.2. Suportar IPSec VPN;

1.1.11.6.3. Suportar SSL VPN;

1.1.11.6.4. A VPN IPSEc deve suportar:

1.1.11.6.5. 3DES, Autenticação MOS e SHA-1, Diffie-Hellman Group 1, Group 2, Group 5 e Group 14, Algoritmo Internet Key Exchange (IKE), AES 128 e 256 (Advanced Encryption Standard) e Autenticação via certificado IKE PKI;

1.1.11.6.6. A solução deve suportar CA Interna e CA Externa de terceiros;

1.1.11.6.7. Solução deve suportar a configuração VPN através de uma interface do tipo GUI (console do fabri cante ou interface web);

1.1.11.7. SOLUÇÃO DE PROTEÇÃO CONTRA AMEAÇAS AVANÇADAS

1.1.11.7.1. A solução deverá prover as funcionalidades de inspeção de artefatos de entrada com malwares não conhecidos ou do tipo APT com filtro de ameaças avançadas e análise de execução em tempo real, sendo essa analise executada na nuvem proprietária do próprio fabricante ou appliance dedicada para sandboxing;

1.1.11.7.2. Prevenir através do bloqueio efetivo do malware desconhecido (Dia Zero), oriundo da comunicação Web (HTTP e HTTPS) e E-mail (SMTP/TLS) via MTA durante análise completa do arquivo no ambiente san dbox, sem que o mesmo seja entregue parcialmente ao cliente.

1.1.11.7.3. A solução deve ser capaz de inspecionar e prevenir malware desconhecido em tráfego criptografado SSL;

1.1.11.7.4. A solução deve fornecer a capacidade de emular ataques em diferentes sistemas operacionais, dentre eles: Windows 7, Windows 8.1 e Windows 10, assim como Office 2003, 2010, 2013 e 20 16;

1.1.11.7.5. Implementar atualização da base de dados de forma automática, permitindo agendamentos diários, dias da semana ou dias do mês assim como o período de cada atualização;

1.1.11.7.6. A solução deve suportar as seguintes topologias de implantação: Inline, Message

Transfer Agent (MTA) e Mirror/TAP;

1.1.11.7.7. A tecnologia de máquina virtual deverá possuir diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso, não sendo baseado apenas em assinaturas;

1.1.11.7.8. A solução de prevença de ameaças avançadas (Sandboxing) contra ataques persistentes e ZeroDay, deve ser habilitada e funcionar de forma independente, ou seja, não sendo obrigatório o uso e ativação de funcionalidades ou engines de anti-virus para a mesma ter o seu devido funcionamento.

1.1.11.7.9. Todas as máquinas virtuais (Windows e pacote Office) utilizadas na solução e solicitadas neste edi tal, devem estar integralmente instaladas e licenciadas, sem a necessidade de intervenções por parte do administrador do sistema. As atualizações deverão ser providas pelo fabricante;

1.1.11.7.10. Para a emulação de arquivos, a solução deve suportar arquivos com tamanho máximo de emulação de até 30Mb.

1.1.11.7.11. Implementar mecanismo de exceção, permitindo a criação de regras por VLAN, subrede e endereço IP;

1.1.11.7.12. Implementar a emulação, detecção e bloqueio de qualquer malware e/ou código malicioso detectado como desconhecido. A solução deve permitir a análise e bloqueio dos seguintes tipos de arquivos caso tenham malware desconhecido: pdf, tar, zip, rar, 7z, exe, rtf, csv, ser, xls, xlsx, xlt, xlm, xltx, xlsm, xltm, xlsb, xla, xlam, xll, xlw, ppt, pptx, pps, pptm, potx, potm, ppam, ppsx, ppsm, doe, docx, dot, doem, dotx, dotm;

1.1.11.7.13. A solução deve permitir a criação de Whitelists baseado no MD5 do arquivo;
1.1.11.7.14. Para melhor administração da solução, a solução deve possibilitar as seguintes

visualizações a nível de monitoração:

1.1.11.7.14.1. Quantidade de arquivos que estão em emulação;

1.1.11.7.14.2. Número de arquivos emulados;

1.1.11.7.15. A solução deve possuir os indicadores abaixo referente ao último dia, última semana ou últimos 30 dias:

1.1.11.7.15.1. Arquivos scaneados;

1.1.11.7.15.2. Arquivos maliciosos;

1.1.12. ITEM 12 - SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO E RELATÓRIOS PARA ATÉ 5 EQUIPAMENTOS

1.1.12.1. Gerência centralizada e relataria para até 5 equipamentos, compatível com os firewalls dos itens 1 à 11 deste TR.

1.1.12.2. A solução de gerência centralizada e relatoria ofertada deve atender aos requisitos técnicos descritos no ANEXO B deste TR.

1.1.13. ITEM 13 - SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO E RELATÓRIOS PARA ATÉ 10 EQUIPAMENTOS

1.1.13.1. Gerência centralizada e relataria para até 10 equipamentos, compatível com os firewalls dos itens 1 à 11 deste TR.

1.1.13.2. A solução de gerência centralizada e relataria ofertada deve atender aos requisitos técnicos descritos no ANEXO B deste TR.

1.1.14. ITEM 14 - SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO E RELATÓRIOS PARA ATÉ 50 EQUIPAMENTOS

1.1.14.1. Gerência centralizada e relataria para até 50 equipamentos, compatível com os firewalls dos itens 1 à 11 deste TR.

1.1.14.2. A solução de gerência centralizada e relataria ofertada deve atender aos requisitos técnicos descritos no ANEXO B deste TR.

1.1.15. ITEM 15 - SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO E RELATÓRIOS PARA ATÉ 150 EQUIPAMENTOS

1.1.15.1. Gerência centralizada e relataria para até 150 equipamentos, compatível com os firewalls dos itens 1 à 11 deste TR.

1.1.15.2. A solução de gerência centralizada e relataria ofertada deve atender aos requisitos técnicos descritos no ANEXO B deste TR.

1.1.16. ITEM 16 - SOLUÇÃO DE NEXT GENERATION ANTI-MALWARE E ANTI-RANSOMWARE COM GERÊNCIA EM NUVEM

1.1.16.1. CARACTERÍSTICAS GERAIS

1.1.16.1.1. É permitida a composição da solução ofertada entre diversos fabricantes, desde que não contemple solução de software livre;

1.1.16.1.2. A solução de proteção avançada para notebooks, desktops e servidores consiste em um agente de segurança que será responsável pela análise de arquivos e comportamentos no sistema operacional do computador do usuário final ou servidor a fim de bloquear qualquer tipo de vulnerabilidade de dia-zero.

1.1.16.1.3. A solução deverá ser gerenciada centralmente através de portal em nuvem fornecido pelo fabricante da solução ou em nuvem privada fornecida pela licitante;

1.1.16.1.4. O acesso ao portal de gerenciamento em nuvem deverá ser seguro, através de HTTPS;

1.1.16.1.5. Deve escanear arquivos e identificar infecções baseado em características comportamentais dos vírus;

1.1.16.1.6. Deve escanear arquivos quando eles forem acessados, executados, permitindo detecção imediata e tratamento por qualquer ameaça;

1.1.16.1.7. Deve permitir executar uma análise detalhada de cada arquivo conforme selecionado pelo usuário;

1.1.16.1.8. Deve permitir especificar diretórios e extensões de arquivos para que sejam excluídos da análise de vírus

1.1.16.1.9. Deve checar as áreas mais comuns do sistema de arquivos e a registry do sistema operacional em busca de ameaças avançadas;

1.1.16.1.10. Deve possuir as seguintes opções de remediação:

1.1.16.1.10.1. Reparar;

1.1.16.1.10.2. Quarentenar;

1.1.16.1.10.3. Apagar;

1.1.16.1.11. Deve permitir ser gerenciado através de console unificada para gerenciamento centralizado de políticas e logs.

1.1.16.1.12. Deve identificar automaticamente o ponto de entrada do malware e o seu impacto para a organização;

1.1.16.1.13. A solução deve suportar os sistemas operacionais:

1.1.16.1.13.1. Windows 7 (32 e 64 bits);

1.1.16.1.13.2. Windows 8.1 (32 e 64 bits);

1.1.16.1.13.3. Windows 10 (32 e 64 bits);

1.1.16.1.13.4. Windows Server 2008 R2 (32 e 64 bits);

1.1.16.1.13.5. Windows Server 2012 R2 (64 bits);

1.1.16.1.13.6. Windows Server 2012 (64 bits);

1.1.16.1.13.7. Windows Server 2016 (64 bits);

1.1.16.1.13.8. Windows Server 2019 (64 bits);

1.1.16.1.14. Deve gerar automaticamente relatório completo da execução do malware utilizando técnicas contidas no MITRE Framework;

1.1.16.1.15. Deve bloquear ataques independentemente se o vetor de distribuição é baseado na web, e-mail ou mídia removível;

1.1.16.1.16. Deve detectar e bloquear comunicações com servidores de comando e controle (C&C) para impedir vazamento de dados mesmo quando conectado/trabalhando remotamente. Deve permitir a quarentena de sistemas infectados para evitar que o malware se espalhe;

1.1.16.1.17. Deve possuir funcionalidade de análise forense de incidente, provendo uma visão completa do fluxo do ataque, causa raiz, impacto no negócio e o ponto de entrada do malware para agilizar as ações de remediação;

1.1.16.1.18. O endpoint deve ser integrado ao antivírus (agente único e gerenciamento), que fornece uma forte proteção de primeira linha estática e dinâmica usando assinaturas e análise comportamental.

1.1.16.1.19. O malware detectado deve ser impedido de baixar (a sessão de download é interceptada pelo en dpoint). Se o malware já estiver na máquina, ele será colocado em quarentena.

1.1.16.1.20. O endpoint deve fornecer a capacidade de ativar e desativar de forma granular cada componente, que serve como um meio para isolar qualquer interferência com outros aplicativos.

1.1.16.1.21. Além das ferramentas de solução de problemas padrão, as informações de forense podem ajudar na identificação de tais interferências;

1.1.16.1.22. Deve ser capaz de efetuar roll-back de mudanças no registro do Windows e alterações no sistema de arquivos em caso de alteração a arquivos infectados;

1.1.16.1.23. Deve proteger os dados forenses armazenados na estação de trabalho (Endpoint) contra acessos não autorizados ou outro tipo de tentativa de manipulação através da estrutura segura de logs da solução;

1.1.16.1.24. Os clientes se comunicam apenas com servidores autorizados (ou seja, apenas IPs específicos fornecidos por um servidor autenticado) e realizam a validação do certificado do servidor (usando informações internas) para verificar se o servidor é confiável;

1.1.16.1.25. Deve possuir análise de campos de login e senha em caso de acesso a páginas internet como email e formulários na detecção e prevenção de sites de phishing;

1.1.16.1.26. Deve possuir proteção contra reuso de credenciais;

1.1.16.1.27. A solução deverá detectar e bloquear em tempo real qualquer tipo de ataque de dia zero;

1.1.16.1.28. A solução deve ser capaz de fazer remediação de forma automatizada, sem a

necessidade da intervenção do usuário;

1.1.16.1.29. A solução deverá detectar e bloquear tem tempo real qualquer ação maliciosa ao sistema operacional que venha através de download de arquivos na Web, cópia através de um drive externo, sites de phishing e até mesmo mecanismos de criptografia de arquivos como o ransomware.

1.1.16.1.30. A solução deve possuir mecanismos de restauração dos arquivos no momento que é detectado e bloqueado o ransomware, ou seja, não permitindo o sequestro de informações.

1.1.16.1.31. A solução deverá detectar e bloquear ameaças em download ou através de movimento lateral (cópia de arquivos) em qualquer extensão Microsoft Office, sendo ela capaz de detectar qualquer tipo de executável que tente criptografar os arquivos do computador do usuário.

1.1.16.1.32. A solução deverá detectar e bloquear malwares dia zero no momento do download e copia através de drive externo. Deve prevenir e remediar de forma automática ataques evasivos de ransomware, baseado em análise comportamental;

1.1.16.1.33. Deve reverter as ações do ransomware, restaurando os dados corporativos automaticamente, garantindo proteção contra criptografia dos dados;

1.1.16.1.34. Possuir tecnologia que não seja baseada apenas em assinaturas, garantindo seu funcionamento tanto de forma online quanto offline;

1.1.16.1.35. Deve permitir que os usuários obtenham políticas e atualizações de uma pasta compartilhada, sem uma conexão com um serviço e gerenciamento.

1.1.16.1.36. Deve implementar, através de análise dinâmica e heurística, proteção em tempo real contra sites conhecidos e desconhecidos de phishing;

1.1.16.1.37. Deve detectar, através de análise estática e heurística, elementos suspeitos em sites que solicitem credenciais dos usuários;

1.1.16.1.38. Deve detectar e prevenir a reutilização de credenciais corporativas em sites externos;

1.1.16.1.39. Deve suportar o monitoramento do Log de Eventos do Windows para analisar eventos de malware de fornecedores de antivírus de terceiros.

1.1.16.1.40. Deve ser capaz de realizar ações com base no Log de Eventos do Windows, como:

1.1.16.1.40.1. Analisar ataques,

1.1.16.1.40.2. Encerrar processos,

1.1.16.1.40.3. Excluir ou colocar arquivos em quarentena

1.1.16.1.41. Deve possuir processo de análise forense automático de incidentes, disponibilizando as seguintes informações sobre o ataque:

1.1.16.1.41.1. Eventos Maliciosos;

1.1.16.1.41.2. Ponto de entrada do malware;

1.1.16.1.41.3. Escopo dos danos causados;

1.1.16.1.41.4. Máquinas infectadas;

1.1.16.2. Gerenciamento Centralizado de políticas de Segurança, Logs e relatórios:

1.1.16.2.1. A gerência dos endpoints deve ser realizada através de console própria ou através de interface web (HTTPS).

1.1.16.2.2. Deve ser capaz de gerenciar todos os endpoint de forma centralizada, possibilitando a concentração dos logs e emissão de relatórios.

1.1.16.2.3. Permitir a criação e distribuição de políticas de segurança de forma centralizada, suportando organização hierárquica de regras em todos os equipamentos.

1.1.16.2.4. A solução deve possuir mecanismo de indexação de logs para permitir uma busca acelerada dos eventos sem a necessidade de abertura de arquivos de logs mais antigos.

1.1.16.2.5. Acesso avançado para monitorar e gerenciar as funções do sistema

1.1.16.2.6. A solução deve ter integração com o Microsoft Active Directory para identificação de usuários

1.1.16.2.7. A solução deve incluir a opção de pesquisar dentro da lista de eventos, drill-down em detalhes para a investigação e análise dos eventos;

1.1.16.2.8. A solução deve apresentar sumario apontando os agentes que estão instalados, em progresso ou que ainda estão pendentes;

1.1.16.2.9. A gerência deve apontar os agentes nos endpoints que foram violados com Segurança;

1.1.16.2.10. Todos os logs deverão ser referenciados com o nome do usuário devido a integração com o Active Directory.

1.1.16.2.11. A solução deve possuir outras funcionalidades de Segurança onde podem ser incorporadas na mesma gerencia.

1.1.16.2.12. Disponibilizar informações gráficas, na linha tempo que informe o número de eventos ocorridos

1.1.16.2.13. Disponibilizar recursos interativos de navegação nos eventos informados;

1.1.16.2.14. A solução deve possuir relatórios customizáveis onde seja possível pegar

diferentes informações para montagem do relatório;

1.1.16.2.15. Correlacionar eventos capaz de utilizar como base informações o número de conexões em determi nado tempo seguido pelo menos das ações:

1.1.16.2.15.1. Bloqueio da origem;

1.1.16.2.15.2. Envio de SNMP;

1.1.16.2.15.3. Envio de e-mail;

1.1.16.2.16. A solução deve exportar relatórios em pelo menos um dos formatos: HTML, CSV e MHT;

1.1.16.2.17. A solução deve possibilitar a visualização geográfica dos eventos de segurança correlacionados;

1.1.16.2.18. A solução deve permitir o administrador ser capaz de atribuir filtros para diferentes linhas do gráfico que são atualizadas em intervalos regulares, mostrando todos os eventos que corresponda a esse filtro. Permitindo ao operador a concentrar-se sobre os eventos mais importantes.

1.1.16.2.19. A solução deve prover no mínimo as seguintes funcionalidades para análise avançada dos incidentes:

1.1.16.2.20. Gráficos com principais eventos de segurança de acordo com a funcionalidade selecionada;

1.1.16.2.21. Estatísticas com comparativo de período (hora, dia e mês);

1.1.16.2.22. Deve permitir a geração de relatórios com horários predefinidos, diários, semanais e mensais. Incluindo principais eventos, principais origens, principais destinos, principais serviços, principais origens e os seus principais eventos, principais destinos e seus principais eventos e

principais serviços e seus principais eventos;

1.1.16.2.23. A solução deve incluir a opção de pesquisar dentro da lista de eventos, drill-down em detalhes para a investigação e análise dos eventos;

1.1.16.2.24. Deve mostrar a distribuição dos diferentes eventos filtrados por país em um mapa, onde deve estar incluso principais eventos de origem ou destino por pais.

1.1.16.2.25. Solução deve ser capaz de detectar ataques de tentativa de login e senha utilizando tipos diferentes de credencias;

1.1.16.2.26. Deve estar inclusa na lista de eventos a opção de gerar automaticamente gráficos ou tabelas com o evento, a origem e distribuição de destino.

1.1.16.2.27. Deve detectar ataques de negação de serviço e correlacionar eventos de todas as fontes.

1.1.16.2.28. Deve estar incluso no dashboard com horários predefinidos, diários, semanais e relatórios mensais. Incluindo:

1.1.16.2.28.1. Top eventos,

1.1.16.2.28.2. Top origem,

1.1.16.2.28.3. Top destinos,

1.1.16.2.28.4. Top Serviços,

1.1.16.2.28.5. Top origens e os seus principais eventos,

1.1.16.2.28.6. Top destinos e seus principais eventos;

1.1.16.2.29. Solução deve incluir relatórios de horários, diários, semanais e mensais pré-definidos. Incluindo pelo menos eventos Top origem, Top destino, Top evento, Top users, Top localidade de origem e os principais eventos relacionados em cada filtro;

1.1.16.2.30. Deve suportar a programação de relatórios automáticos, para as informações básicas que precisa extrair de forma diária, semanal e mensal. Também deve permitir ao administrador definir a data e a hora que o sistema de informação começa a gerar o relatório agendado.

1.1.17. ITEM 17 - SOLUÇÃO DE PROTEÇÃO PARA DISPOSITIVOS MÓVEIS ANDROID E IOS

1.1.17.1. CARACTERÍSTICAS GERAIS

1.1.17.1.1. A solução deve ser capaz de proteger ameaças de diferentes vetores de ataque, como pelo menos:

1.1.17.1.1.1. Infecção de Malware;

1.1.17.1.1.2. Ataques de Phishing;

1.1.17.1.1.3. Documentos maliciosos;

1.1.17.1.1.4. Ameaças de rede;

1.1.17.1.1.5. Alterações ao sistema operacional sem o aviso prévio ao usuário;

1.1.17.1.2. A solução deve detectar ameaças conhecidas e desconhecidas, incluindo aplicações consideradas de alto risco;

1.1.17.1.3. A solução deve prevenir o acesso a links maliciosos;

1.1.17.1.4. A solução de prevenir ataques do tipo phishing e zero-phising (phishing zero-day);
1.1.17.1.5. A solução deve alertar e bloquear características de side-loading (carregamento em paralelo de aplicações);

1.1.17.1.6. Suporte para dispositivos BYOD e dispositivos gerenciados dentro da organização; A

solução deve suportar os sistemas operacionais Android e iOS;

1.1.17.1.7. O gerenciamento da solução deve disponibilizar recursos de avaliação de risco completa;

1.1.17.1.8. O gerenciamento da solução deve disponibilizar ao administrador da solução um dashboard que demonstre, pelo menos:

1.1.17.1.8.1. O status do risco dos dispositivos

1.1.17.1.8.2. Status da proteção;

1.1.17.1.8.3. Eventos e alertas recentes;

1.1.17.1.9. A solução deve prover opções de remediação e mitigação caso uma ameaça seja detectada;

1.1.17.2. REQUISITOS DE DETECÇÃO

1.1.17.2.1. Proteger o dispositivo de aplicações maliciosas conhecidas e desconhecidas.

1.1.17.2.2. Analisar o comportamento real dos aplicativos.

1.1.17.2.3. Detectar e analisar o aplicativo baseado na reputação do desenvolvedor.

1.1.17.2.4. Permitir o Whitelist e Blacklist de aplicações.

1.1.17.2.5. Prover indicadores de severidade para ameaças identificadas.

1.1.17.2.6. Prover um SLA (tempo necessário para a detecção de um malware) no momento da sua instalação.

1.1.17.2.7. A solução deve detectar comunicações comprometidas e tráfego de rede anômalo do dispositivo e para o dispositivo. (Ex. Man-in-The-Middle attack MiTM)

1.1.17.2.8. Detecção de interceptação SSL (Ex. SSL string & SSL Bump)

1.1.17.2.9. Deve possuir habilidade para realizar o Whitelist de certificados.

1.1.17.2.10. Deve possuir habilidade para configurar URL filter e bloquear o acesso ao recurso quando o dispositivo estiver em risco.

1.1.17.2.11. Deve possuir habilidade para bloquear o acesso para links maliciosos / sites utilizados para Phishing.

1.1.17.2.12. Deve prover uma navegação segura para o usuário e bloquear links maliciosos. OS & Exploração do Dispositivo o Detectar vulnerabilidades e exploits conhecidos dos dispositivos mobile.

1.1.17.2.13. Detectar dispositivos Android com Root e dispositivos iOS com Jailbroken habilitados.

1.1.17.2.14. Detectar ferramentas de evasão para Jailbreak/Root.

1.1.17.2.15. Alertar sobre exploração de vulnerabilidades utilizando Bluetooth.

1.1.17.2.16. Detectar configurações de sistema operacional que podem causar risco para o dispositivo.

1.1.17.2.17. Prevenir mensagens de SMS/Texto que contenham links de phishing.

1.1.17.2.18. Alertar versões de sistema operacional (OS) desatualizados.

1.1.17.2.19. Recursos de anti-bot com a capacidade de bloquear malware de realizar acessos a sites, IP e Ser vidores de C&C maliciosos conhecidos.

1.1.17.2.20. Bloquear a instalação de profiles de configuração para iOS e permitir a configuração de realizar Whitelist de Profiles.

1.1.17.2.21. Proteção para aplicativos em execução paralela (background):

1.1.17.2.22. Gerar alerta no iOS para a aprovação de certificado assinado de desenvolvedor.
1.1.17.2.23. Habilidade de forçar o scan em aplicativos Android e realizar o bloqueio do APK caso seja identifi cada como malicioso.

1.1.17.2.24. Bloquear o download de IPA ou APK (baseado em políticas)

1.1.17.2.25. Disponibilizar pelo menos 3 níveis de classificação de risco para o dispositivo.
1.1.17.2.26. A solução deve minimizar a identificação de falso positivo (atribuir risco baixo para aplicativos válidos).

1.1.17.3. REQUISITOS DE MITIGAÇÃO DE AMEAÇAS

1.1.17.3.1. A solução deve suportar a notificação do usuário e solicitar que o usuário escolha uma ação, como deletar o aplicativo malicioso, deletar mensagens de texto de phishing ou desconectar o dispositivo da rede quando uma ameaça for detectada.

1.1.17.3.2. A solução deve integrar com soluções de terceiros de UEM/MDM/EMM que permita ações de remediação para o dispositivo. (ex: remoção de dados da corporação, quarentena de dispositivos, bloquear o acesso a recursos da organização).

1.1.17.3.3. A solução deve ter suporte para bloquear o acesso aos recursos da corporação, quando o dispositivo se encontrar comprometido ou quando o usuário tentar efetuar a desinstalação da proteção.

1.1.17.3.4. A solução deve oferecer a proteção contra ameaças de rede e efetuar o bloqueio a site maliciosos.

1.1.17.3.5. A solução deve bloquear a comunicação com sites de C&C quando identificado o Malware.

1.1.17.3.6. A solução deve fornecer suporte para filtro de conteúdo, com bloqueio baseado em categorias para impedir o acesso a sites não autorizados.

1.1.17.4. REQUISITOS DE INSTALAÇÃO

1.1.17.4.1. Suporte para a última versão disponível de sistema operacional Android e iOS;
1.1.17.4.2. O aplicativo deve estar disponibilizado nas lojas oficiais App Store e Google Play.
1.1.17.4.3. Não permitir alterações na configuração do aplicativo realizadas pelo usuário.

1.1.17.4.4. Dar suporte para ativação e inicialização remota do aplicativo.

1.1.17.4.5. Suporte para instalação de aplicativos customizados pela corporação, assinados para iOS.

1.1.17.5. VISIBILIDADE

1.1.17.5.1. A solução deve prover total visibilidade e controle sobre os eventos de segurança, e alterações no status do dispositivo.

1.1.17.5.2. Deve possuir Hhbilidade de conduzir investigações para garantir a aplicação de políticas de segurança contendo as seguintes categorias:

1.1.17.5.2.1. OS/Dispositivo

1.1.17.5.2.2. Aplicativos

1.1.17.5.2.3. Rede

1.1.17.5.3. A solução deve integrar com soluções de SIEM, suportar o export de logs de Segurança através de Syslog / Remate Syslog.

1.1.17.6. GERENCIAMENTO E ADMINISTRAÇÃO

1.1.17.6.1. Possuir um console de gerenciamento unificado;

1.1.17.6.2. Possuir suporte ao acesso ao console de gerenciamento através de interface web, suportando os navegadores comuns do mercado.

1.1.17.6.3. Deve possuir configuração de perfis de administrador.

1.1.17.6.4. A solução deve oferecer suporte granular de configurações através de políticas. O licenciamento deve ser feito por dispositivo protegido;

1.1.17.6.5. A conexão com a console de gerenciamento deve ser feita através de um protocolo seguro. (Ex: SSL)

1.1.17.6.6. Habilidade de adicionar ou remover dispositivos, e atribuir a diferentes grupos.
1.1.17.6.7. Deve permitir que administradores realizem o upload de um arquivo APK (formato Android App) na console de gerenciamento e gerar um relatório completo de análise do aplicativo

1.1.17.6.8. Permitir a customização do e-mail enviado para os usuários para a instalação e configuração da solução.

1.1.17.6.9. Deve registrar em logs de auditoria todas as operações dos administradores.

1.1.17.6.10. Suportar configuração de MFA (Multi Factor Authentication) para o login de administradores a console de gerenciamento.

1.1.17.6.11. A solução deve suportar integração com soluções MDM / EMM / UEM;

1.1.17.6.12. A lista de dispositivos a serem provisionados pode ser definida no MDM e lida pela solução;

1.1.17.6.13. A solução deve listar de dispositivos por agrupamento, conforme apresentado no MDM (por exem plo, estrutura organizacional/ etiquetas/ etc.);

1.1.17.6.14. Deve ter a capacidade de bloquear informações pessoais de funcionários do MDM visando privacidade;

1.1.17.7. RELATÓRIOS E ALERTAS

1.1.17.7.1. Deve exibir informações sobre a última conexão do agente com a console de gerenciamento por dispositivo.

1.1.17.7.2. Deve exibir informações sobre o status de provisionamento de cada dispositivo.
1.1.17.7.3. Deve exibir informações sobre versão do software instalado de cada dispositivo.
1.1.17.7.4. Deve exibir o número total de dispositivos com o agente instalado na organização.
1.1.17.7.5. Deve exibir informação sobre os riscos atuais encontrados no dispositivo.

1.1.17.7.6. Deve exibir informações sobre os tipos de riscos e suas categorias.

1.1.17.7.7. Deve possuir opção de drill down para a investigação de um alerta específico;
1.1.17.7.8. Deve possuir alertas de eventos de segurança classificados pelo tipo.

1.1.17.7.9. Deve possuir alertas de eventos de segurança em filtros diferentes (hora/dia/etc.)
1.1.17.7.10. Deve possuir habilidade para enviar SMS e e-mail para o administrador referente aos eventos de segurança.

1.1.17.7.11. Deve permitir a configuração de relatórios agendados de forma diária, semanal ou mensal.

1.1.17.8. PRIVACIDADE E DESEMPENHO

1.1.17.8.1. A solução não deve invadir a privacidade do usuário os dados do aplicativo que são privados para o usuário não devem ser enviadas ou gravadas.

1.1.17.8.2. Essas informações incluem, mas não se limitam a: mensagens de texto, arquivos de

foto/ voz/ ví deo do dispositivo, outros documentos, e-mails, contatos, eventos da agenda e localização;

1.1.17.8.3. A solução não deve enviar e armazenar informações de identificação pessoal (PII) para servidores de análise em texto não criptografado;

1.1.17.8.4. A solução deve ter a capacidade de ocultar a lista de aplicativos por dispositivo por usuário;

1.1.17.8.5. A solução poderá desativar o rastreamento de localização do dispositivo em ataques à rede por política do cliente;

1.1.17.8.6. A solução deve ter a capacidade de desativar a leitura de SMS durante ataques de smishing de acordo com a política do cliente;

1.1.17.8.7. A solução deve permitir gerenciar políticas de segurança por modelo e permitir políticas diferentes para diferentes grupos de dispositivos;

1.1.17.8.8. A solução deve fornecer proteção sem comprometer a experiência do usuário e o desempenho do dispositivo (por exemplo: não intrusivo, baixo uso de bateria e baixo uso de rede)

1.1.17.8.9. A solução deve minimizar o upload de aplicativos para o servidor de análise se o dispositivo estiver usando a rede móvel;

1.1.17.9. REQUISITOS DE SEGURANÇA

1.1.17.9.1. A arquitetura da solução deve garantir que nenhuma informação privada de dispositivos e usuários (usuário, nome, e-mail e números de telefone) seja exposta;

1.1.17.9.2. Todos os protocolos de comunicação entre servidor e cliente devem ser criptografados;

1.1.17.9.3. Nomes de usuário e senhas armazenados devem ser criptografados;

1.1.17.9.4. Deve possuiar a capacidade de integração com o Active Directory da organização e permitir acesso SSO (logon único) para os administradores;

1.1.18. ITEM 18 – SOLUÇÃO DE PREVENÇÃO DE AMEAÇAS E SPAM PARA E-MAIL EM NUVEM – MICROSOFT 365 E GOOGLE WORKSPACE

1.1.18.1. CARACTERISTICAS GERAIS

1.1.18.1.1. A solução deve possuir mecanismos de proteção multi-camadas contra as ameaças em serviços de e-mail em nuvem (SaaS):

1.1.18.1.1.1. Prevenção de ameaças avançadas (APT) ou dia zero (zero day);

1.1.18.1.1.2. Proteção contra phishing;

1.1.18.1.1.3. Possibilidade de identificar e-mails de spam;

1.1.18.1.1.4. Análise e detecção de vazamento de dados (DLP);

1.1.18.1.1.5. Gerar visibilidade de aplicações SaaS não autorizadas (Shadow IT);

1.1.18.1.1.6. Integração nativa com aplicações SaaS: Microsoft 365 e Google Workspace;

1.1.18.1.1.7. Arquitetura unificada para visibilidade de logs e gerenciamento de políticas;

1.1.18.1.1.8. Limpeza e extração contra conteúdo malicioso em anexos (CDR);

1.1.18.1.2. Fazer integração via API da ferramenta de segurança para aplicações SaaS;

1.1.18.1.3. Durante integração deve fazer query na base de dados de usuários sem a necessidade de agentes para ter visibilidade dos usuários e grupos;

1.1.18.1.4. Durante a integração inicial com o Microsoft 365, deve ser possível determinar qual grupo ou usuários farão parte das políticas de segurança para inspeção dos e-mails e outras

aplicações SaaS;

1.1.18.1.5. A solução de prevenção de ameaças avançadas, deve possuir funcionalidades de sandboxing, antivírus, reputação de URL e anti-phishing;

1.1.18.1.6. Nas configurações de políticas de segurança, deve possuir as opções de detectar e prevenir;

1.1.18.1.7. Deve identificar os grupos ou usuários que serão inspecionados e ter uma lista de exclusão baseado na conta do Microsoft 365;

1.1.18.1.8. Criação de alertas para administradores da ferramenta para qualquer malware identificado, assim como phishing. Tornando também opcional o alerta do usuário de destino sobre possíveis malwares;

1.1.18.1.9. A solução de sandboxing, deve ser na nuvem do próprio fabricante, sendo ela proprietária;

1.1.18.1.10. A funcionalidade de análise de ameaças avançadas e de dia zero deve implantar mecanismo de sandboxing resistente a evasões;

1.1.18.1.11. Na solução de prevenção de ameaças avançadas, deve apresentar nos logs as seguintes informações:

1.1.18.1.11.1. Todas as funcionalidades de segurança que identificaram a ameaça;

1.1.18.1.11.2. Nome do arquivo identificado;

1.1.18.1.11.3. Deve informar o MD5, SHA-1 e SHA-256 para fazer pesquisas e comparar com outras fontes de terceiro. Ex.: Virus Total;

1.1.18.1.11.4. Dentro do log, deve possuir link onde é possivel em um click direcionar a pesquisa do arquivo ou URL direto no virus total;

1.1.18.1.11.5. Quando detectado e bloqueado algum arquivo ou URL maliciosa, deve permitir que o administrador consulte através da plataforma externa do “Virus total” (www.virustotal.com) se alguma engine de Antivirus baseada em assinatura é capaz de identificar o ataque apontado pela ferramenta de prevenção de ameaças.

1.1.18.1.11.6. Identificar o usuário que recebeu o e-mail malicioso;

1.1.18.1.12. Cada log de sandboxing, quando identificada uma ameaça, deve apresentar informações detalhadas do arquivo malicioso para análise:

1.1.18.1.12.1. Tamanho do arquivo;

1.1.18.1.12.2. Tipo do arquivo;

1.1.18.1.12.3. Lista de hash que o arquivo possui;

1.1.18.1.12.4. Veredito do ataque;

1.1.18.1.12.5. Risco de segurança;

1.1.18.1.12.6. Nível de confiança;

1.1.18.1.12.7. Classificação do ataque, ou seja, se é uma familia já conhecida. Ex.: Trojan;

1.1.18.1.12.8. Apresentar no próprio relatório o malware identificado, evidências do ataque já no Framework do MITRE ATT&CK, classificando as devidas táticas e técnicas do ataque;

1.1.18.1.12.9. Lista dos arquivos encontrados dentro o malware identificado. Ex.: Pode ser um arquivo ZIP com outros arquivos ou executáveis que possuem outros arquivos associados a ele;

1.1.18.1.12.10. Atividades suspeitas no computador do Sandboxing que vai simular a ação humana como: eventos no file system, chave de registro, eventos de rede apresentando possiveis URL’s ou IP’s.

1.1.18.1.12.11. Vídeo da máquina virtual dentro da solução de Sandboxing, apresentando o comportamento humano;

1.1.18.1.13. A solução, deve possuir engine onde no momento que encontrado um conteúdo malicioso no arquivo office ou PDF, a mesma deve reconstruir o arquivo removendo o conteúdo malicioso, sendo capaz de converter arquivos reconstruídos para o formato PDF para melhor segurança, ou manter-se em formato original de acordo com política estabelecida.

1.1.18.1.14. Deve possuir console de gerenciamento web na nuvem, sem a necessidade de infraestutura específica e já incluída nos custos de licenciamento da solução.

1.1.18.1.15. Deve inspecionar todos os arquivos em tempo real nos serviços SaaS de e-mail, verificando a presença de malwares ou dados sensíveis.

1.1.18.1.16. Deve inspecionar todos os arquivos previamente existentes com no mínimo de 7 dias retroativos à data inicial da integração dos serviços SaaS de e-mail, verificando a presença de malwares;

1.1.18.1.17. Toda integração deve ser feita através de API, sem a necessidade de integração com nenhuma solução de proxy local ou agentes.

1.1.18.1.18. Deve possuir integração nativa com a nuvem de inteligência de ameaças (Threat Intelligence) do fabricante para prevenção de ameaças e checagem de reputação.

1.1.18.1.19. Identificar nos e-mails phishing e apresentar os seguintes parâmetros nos eventos:

1.1.18.1.19.1. Remetente;

1.1.18.1.19.2. Destinatário;

1.1.18.1.19.3. Destinatários copiados;

1.1.18.1.19.4. Título do e-mail;

1.1.18.1.19.5. Tipo de conteúdo, exemplo HTML;

1.1.18.1.19.6. Data e horário do recebimento do e-mail;

1.1.18.1.19.7. Alias do usuário;

1.1.18.1.19.8. Quando identificado um phishing, deve apresentar informações como:

1.1.18.1.19.9. Indicadores da detecção como phishing:

1.1.18.1.19.10. Análise do ataque;

1.1.18.1.19.11. Reputação de quem enviou;

1.1.18.1.19.12. Nível de confiança para determinar se é alto ou não;

1.1.18.1.19.13. Informações que são identificadas no cabeçalho do e-mail como falta do DMARC e assinatura DKIM

1.1.18.1.20. Caso tenha alguma URL no corpo do e-mail que foi caracterizada como phishing, a mesma deve ser apresentada nos logs;

1.1.18.1.21. A solução deverá realizar análise dos links enviados no corpo do e-mail. Essa análise deverá apresentar o motivo do porquê foi caracterizado como suspeito ou malicioso.

1.1.18.1.22. A solução deve apresentar uma visualização prévia da URL suspeita.

1.1.18.1.23. O administrador deve ter a opção de solicitar na ferramenta a reclassificação referente a um evento de prevenção de ameaças que não corresponde ao log apresentado.

1.1.18.1.24. Deverá prover mecanismo de proteção para links, onde a solução deverá validar a URL antes de redirecionar para o usuário.

1.1.18.1.25. Pesquisar no log do evento de phishing, outros e-mails baseados no ataque recebido

que possuam os mesmos critérios como quem enviou, título de e-mail e outros tópicos;

1.1.18.1.26. A solução deverá apresentar quais os indicadores que a Inteligência Artificial identificou e caracterizou o evento.

1.1.18.1.27. Solução de DLP, deve criar regras granulares baseada em escopo de e-mail e deve permitir selecionar os tipos de dados que serão usados na política;

1.1.18.1.28. Deve permitir a criação de tipo de dado customizado baseado em expressão regular, template, dicionário de palavras e outros;

1.1.18.1.29. O mecanismo de DLP deverá ter capacidade de detectar informações sensíveis entre todas as plataformas SaaS integradas, com pelo menos as soluções Microsoft 365 e Google Workspace.

1.1.18.1.30. Relatório sumarizado contendo todas as funcionalidades de segurança;

1.1.18.1.31. Listar a quantidade de objetos escaneados e a quantidade de ameaças

identificadas;

1.1.18.1.32. Possuir mecanismo de quarentena onde o administrador consegue visualizar todos os e-mails que foram identificados como maliciosos;

1.1.18.1.33. Permitir a restauração do e-mail em quarentena através da ferramenta;

1.1.18.1.34. Deverá permitir que o usuário solicite a liberação de um e-mail em quarentena.
1.1.18.1.35. Visibilidade dos eventos através de usuários que estão integrados na ferramenta

de forma automática;

1.1.18.1.36. Deve ser possível selecionar o usuário e identificar todos os eventos de segurança baseado por perído e funcionalidade de segurança;

1.1.18.1.37. Visibilidade correlacionada de todos os eventos de segurança.

1.1.18.1.38. Deve inspecionar todos os arquivos previamente existentes nos serviços SaaS após a integração inicial, seja em e-mail ou compartilhamento de arquivos, verificando a presença de malwares ou dados sensíveis.

1.1.18.1.39. Deve identificar tentativas de acesso anômalas aos serviços SaaS, tal como o acesso simultâneo com uma mesma credencial a partir de localizações geograficamente distantes.

1.1.18.2. GERENCIAMENTO E VISIBILIDADE

1.1.18.2.1. Deve possuir uma dashboard que permita ao administrador de segurança ter visibilidade consolidada das ameaças identificadas nos diferentes serviços SaaS, incluindo eventos de malware, URLs maliciosas, phishing, Shadow IT e DLP.

1.1.18.2.2. Deve prover uma interface para visualização detalhada dos eventos maliciosos identificados nos serviços SaaS.

1.1.18.2.3. A solução deverá ser capaz de oferecer integração com ferramentas de SIEM tanto on-premise quanto em nuvem, oferecendo no mínimo Splunk, AWS e Azure Log.

1.1.18.2.4. Deve ser possível especificar o serviço SaaS afetado, o vetor de entrega da ameaça e o detalhamento das ações de mitigação adotadas.

1.1.18.2.5. A gerência centralizada deve permitir visibilidade sumarizada de todas as atividades maliciosas identificadas pela solução de diferentes funcionalidades suportadas pela ferramenta como: Malwares, Phishing, DLP, Shadow IT e anomalias. Sendo possível fazer drill-drow e navegar nos logs para análise das atividades suspeitas.

1.1.18.2.6. Deve possuir gráficos e filtros que permitam ao administrador identificar rapidamente as ameaças identificadas nos serviços SaaS.

1.1.18.2.7. A gerência centralizada deve permitir visualizar a quantidade de usuários que estão ativos na solução de e-mail, assim como a quantidade de e-mails e arquivos inspecionados;

1.1.18.2.8. Deve possuir relatórios analíticos com as estatísticas dos serviços SaaS utilizados, incluindo quantidade de usuários do serviço, volume de e-mails, volume de arquivos e os respectivos eventos maliciosos por funcionalidade de proteção.

1.1.18.2.9. A solução deve fornecer relatórios de atividades para cada aplicação SaaS (Microsoft 365 e Google Workspace);

1.1.18.2.10. Deve dispor de sumário total de risco identificados no Microsoft 365, entre eles:

1.1.18.2.10.1. DLP;

1.1.18.2.10.2. Malware;

1.1.18.2.10.3. Phishing;

1.1.18.2.10.4. Anomalia;

1.1.18.2.10.5. Malwares suspeitos;

1.1.18.2.10.6. Phishing suspeitos;

1.1.18.2.10.7. Spam;

1.1.18.2.10.8. Shadow IT;

1.1.18.2.11. Deve permitir a configuração de políticas independentes para cada serviço SaaS. 1.1.18.2.12. Deve permitir múltiplas regras de segurança para cada serviço SaaS, aplicando

proteções diferenciadas baseados em usuários ou grupos de usuários

1.1.18.2.13. Quando identificado um evento na solução Prevenção de ameaças, o administrador deve ter as seguintes opções de ação baseado em cada log:

1.1.18.2.13.1. Alertar o usuário sobre a ameaça;

1.1.18.2.13.2. Liberar o arquivo inspecionado e bloqueado;

1.1.18.2.13.3. Reportar para o fabricante que não é um arquivo malicioso;

1.1.18.2.13.4. Desconsiderar evento;

1.1.18.2.13.5. Analisar o relatório do incidente.

1.1.18.2.14. As regras devem permitir a geração de alertas por email para os administradores para os casos de malware, phishing e DLP, bem como a customização das mensagens de alerta;

1.1.18.2.15. Quando identificado um evento de phising, o administrador deve ter as seguintes opções de ação:

1.1.18.2.15.1. Categorizar como SPAM; 1.1.18.2.15.2. Alertar usuários que é um phishing; 1.1.18.2.15.3. Quarentenar e-mail;

1.1.18.2.15.4. Criar exceção.

1.1.18.2.16. Quando identificado um evento de Anomalia, o administrador deve ter as seguintes opções de ação:

1.1.18.2.16.1. Desconsiderar evento;

1.1.18.2.16.2. Adicionar exceção a partir do evento.

1.1.18.2.17. Quando identificado um evento na solução de ShadowIT, o administrador deve ter as seguintes opções:

1.1.18.2.17.1. Aprovar aplicação;

1.1.18.2.17.2. Desconsiderar evento.

1.1.18.2.18. A solução deve possuir painel de Quarentena baseado nas aplicações SaaS, Microsoft 365, permitindo o administrador ter acesso aos itens que foram colocados em quarentena;

1.1.18.2.19. A quarentena deve permitir que o administrador possa tomar ação para as requisições de restauração do e-mail Microsoft 365.

1.1.19. ITEM 19 – FIREWALL DE APLICAÇÃO WEB – WAF – VIRTUAL

1.1.19.1. A solução de Firewall de Aplicação Web (WAF) deverá ser fornecida na forma de appliance virtual. Devem estar inclusas todas as licenças e garantias necessárias para sua instalação, configuração e operação

1.1.19.2. Deve ser fornecido em appliance virtual compatível com no mínimos os seguintes hypervisors:

1.1.19.2.1. VMware ESX/ESXi 5.5/6.0/7.0;

1.1.19.2.2. Microsoft Hyper-V 2008 R2/2012/2012 R2/2016/2019/2022;

1.1.19.3. Deve suportar instalação em ambiente de alta disponibilidade;

1.1.19.4. Ser capaz de operar em modo Ativo/Standby;

1.1.19.5. Ser capaz de operar em modo Ativo/Ativo, mantendo o status das conexões. Aceita-se como Ativo/Ativo a utilização de dois endereços Virtuais, onde cada endereço fica ativo em um elemento e standby no outro;

1.1.19.6. Suportar a operação da solução de 02 (dois) ou mais appliances, quando implementada em ambiente redundante, suporte sincronismo de sessão entre os dois membros. A falha do equipamento principal não deverá causar a interrupção das sessões balanceadas;

1.1.19.7. Fornecer todos os recursos possíveis de redundância sem nenhuma despesa com licenças adicionais;

1.1.19.8. A solução deve possuir escalabilidade, podendo incrementar sua capacidade de processamento através de licenças;

1.1.19.9. Deve ser fornecido com licenciamento que habilite o throughput mínimo de 1 Gbps.

1.1.19.10. Possuir recurso para o transporte de múltiplas VLANs por uma única porta (ou por um conjunto agregado de portas) utilizando o protocolo 802.1q;

1.1.19.11. Analisar e proteger tráfego HTTP/1.0, HTTP/1.1, HTTP/2.0 e/ou HTTP/3;

1.1.19.12. Possuir suporte a IPv6;

1.1.19.13. A solução deve permitir o encapsulamento, em camada 3, do tráfego entre o balanceador e o servidor para tráfego IPv4 e IPv6, quando o balanceamento é realizado apenas em direção ao servidor, onde a resposta do servidor real é enviada diretamente ao cliente;

1.1.19.14. Possuir suporte à funcionalidade de VXLAN para integração com o ambiente de virtualização (Software Defined Network);

1.1.19.15. Assinar cookies digitalmente e editar endereços de URL (“URL Rewriting”);

1.1.19.16. Os usuários de gerência deverão poder ser autenticados em bases remotas. No mínimo RADIUS, LDAP e TACACS+ deverão ser suportados;

1.1.19.17. Deverá possuir uma funcionalidade de criação automática de políticas, para proteção DDOS e ataques zero-day onde a política de segurança é criada e atualizada automaticamente baseando-se no tráfego real observado à aplicação;

1.1.19.18. Restringir métodos HTTP/ HTTPS permitidos, tipos ou versões de protocolos, tipos de

caracteres e versões utilizadas de cookies;

1.1.19.19. Permitir as seguintes opções de implementação:

1.1.19.19.1. Monitoramento (sem bloqueio);

1.1.19.19.2. Proxy (reverso e transparente);

1.1.19.20. Permitir que novas políticas fiquem apenas monitorando o tráfego, sem bloqueá-lo, indicando caso aconteça algum evento;

1.1.19.21. Remover as mensagens de erro do conteúdo que será enviado aos usuários;

1.1.19.22. Proteger contra-ataques automatizados, incluindo bots e web scraping, identificando comportamento não humano, navegadores operados por scripts ou qualquer outra forma que não operados por humanos;

1.1.19.23. Possuir firewall XML integrado com suporte a filtro e validação de funções XML específicas da aplicação;

1.1.19.24. A solução deve suportar e fazer a proteção do tráfego de protocolo WebSocket;

1.1.19.25. Permitir a utilização de modelo positivo de segurança para proteger contra ataques às aplicações HTTP e HTTPS, além de proteção contra-ataques conhecidos aos protocolos HTTP e HTTPS;

1.1.19.26. Criação de políticas automáticas que bloqueiam o endereço IP que realizar violações;

1.1.19.27. Possuir mecanismo de aprendizado automatizado capaz de identificar todos os conteúdos das aplicações, incluindo URLs, parâmetros URLs, campos de formulários, o que se espera de cada campo (tipo de dado, tamanho de caracteres, se é um campo obrigatório), cookies, ações SOAP e elementos XML. Identificar e criar perfil de utilização dos aplicativos, inclusive desenvolvidos em Javascript, CGI, ASP e PHP;

1.1.19.28. Deve possuir tecnologia para mitigação de DDoS em camada 7 baseado em análise comportamental, usando o aprendizado;

1.1.19.29. A solução deve possuir a capacidade de capturar tráfego no formato TCP Dump relativos a ataques DoS L7, Web Scraping e força bruta permitindo uma análise mais aprofundada por parte do administrador;

1.1.19.30. Detectar ataques de força bruta por meio dos seguintes métodos:

1.1.19.30.1. Aumento do tempo de resposta da aplicação monitorada ou bloqueio temporário do atacante;

1.1.19.30.2. Quantidade de transações por segundo (TPS), monitorando a quantidade de transações por segundo por endereço IP;

1.1.19.31. Permitir a criação de políticas diferenciadas por aplicação e por URL, onde cada aplicação e URL poderão ter políticas totalmente diferentes;

1.1.19.32. Apresentar proteção contra-ataques, como:

1.1.19.32.1. Brute Force Login;

1.1.19.32.2. Buffer Overflow;

1.1.19.32.3. Cookie Injection;

1.1.19.32.4. Cookie Poisoning;

1.1.19.32.5. Cross Site Request Forgery (CSRF);

1.1.19.32.6. Cross Site Scripting (XSS);

1.1.19.32.7. Server Side Request Forgery (SSRF); 1.1.19.32.8. Directory Traversal;

1.1.19.32.9. Forceful Browsing;

1.1.19.32.10. HTTP Denial of Service;

1.1.19.32.11. HTTP hidden field manipulation;

1.1.19.32.12. HTTP request smuggling;

1.1.19.32.13. HTTP Response Splitting;

1.1.19.32.14. Malicious Robots;

1.1.19.32.15. Parameter Tampering;

1.1.19.32.16. Remote File Inclusion Attacks;

1.1.19.32.17. Sensitive Data Leakage (Social Security Numbers, Cardholder Data, PII, HPI);
1.1.19.32.18. Session Hijacking;

1.1.19.32.19. SQL Injection;

1.1.19.32.20. Web Scraping;

1.1.19.32.21. Web server software and operating system attacks;

1.1.19.32.22. Web Services (XML) attacks;

1.1.19.33. Deve permitir que possa ser especificado na política os tipos de arquivos que serão bloqueados (File Types);

1.1.19.34. A solução deve permitir a inspeção de upload de arquivos para os servidores de aplicação, ou enviar para inspeção através do protocolo ICAP;

1.1.19.35. Deve encriptar dados e credenciais na camada de aplicação, sem ter a necessidade de atualizar a aplicação. Essas informações devem ser encriptadas para proteger o login e as credenciais dos usuários e com isso os dados da aplicação;

1.1.19.36. Deve proteger informações sensíveis e confidenciais da interceptação por terceiros, através da criptografia de dados quando ainda no browser do usuário. Deve proteger esses dados criptografados de malwares e keyloggers;

1.1.19.37. Deve ofuscar o nome de um parâmetro sensível da aplicação em caracteres randômicos. Esse nome de parâmetro deve ser mudado constantemente pela ferramenta para dificultar ataques direcionados;

1.1.19.38. A solução deve fornecer relatórios consolidados de ataques com pelo menos os seguintes dados:

1.1.19.38.1. Resumo geral com as políticas ativas, anomalias e estatísticas de tráfego, Ataques DoS, Ataques de Força Bruta, Ataques de Robôs, Violações, URL, Endereços IP, Países, Severidade;

1.1.19.39. Deverá permitir o agendamento de relatórios a serem entregues por email;

1.1.19.40. Emitir os seguintes relatórios gráficos por:

1.1.19.40.1. Política de segurança;

1.1.19.40.2. Tipos de ataques;

1.1.19.40.3. Violações;

1.1.19.40.4. URL que foram atacadas;

1.1.19.40.5. Endereços IP de origem;

1.1.19.40.6. Localização geográfica dos endereços IPs de origem;

1.1.19.40.7. Severidade;

1.1.19.40.8. Código de resposta;

1.1.19.40.9. Métodos;

1.1.19.40.10. Protocolos;

1.1.19.40.11. Sessão;

1.1.19.41. A solução deve ser capaz de proteger GraphQL APIs com pelos menos os seguintes parâmetros: tamanho total, tamanho de cada parâmetro

1.1.19.42. A solução deve ser capaz de proteger GraphQL APIs limitando a quantidade de queries dentro de uma requisição HTTP

1.1.19.43. A solução deve ser capaz de proteger APIs baseadas em OpenAPI 2.0

1.1.19.44. A solução deve ser capaz de proteger APIs baseadas em OpenAPI 3.0

1.1.19.45. A solução deve suportar a criação de políticas de proteção com base no modelo OWASP, onde pelo menos devem ser aplicadas políticas de proteção contra o TOP 10 OWASP

1.1.19.46. A solução deve emitir relatório com análise cada política de proteção comparado com o TOP 10 OWASP.

1.1.19.47. A solução deverá possuir as seguintes formas de detecção de ataques DoS na camada de aplicação:

1.1.19.47.1. Número de requisições por segundo enviados a uma URL específica;

1.1.19.47.2. Número de requisições por segundo enviados de um IP específico;

1.1.19.47.3. Detecção através de código executado no cliente com o objetivo de detectar interação humana ou comportamento de robôs (bots);

1.1.19.47.4. Número máximo de transações por segundo (TPS) de um determinado IP;

1.1.19.47.5. Aumento de um determinado percentual do número de transações por segundo (TPS);

1.1.19.47.6. Aumento do stress do servidor de aplicação;

1.1.19.48. Funcionalidades de Balanceamento de Carga

1.1.19.48.1. Deve suportar todas as aplicações comuns de um Switch Layer 7, como:

1.1.19.48.1.1. Server Load-Balancing;

1.1.19.48.1.2. Firewall Load-Balancing;

1.1.19.48.1.3. Proxy Load-Balancing;

1.1.19.48.2. Deve suportar balanceamento apenas em direção ao servidor, onde a resposta do servidor real é enviada diretamente ao cliente;

1.1.19.48.3. Deve permitir o encapsulamento, em camada 3, do tráfego entre a solução e o servidor para tráfego IPv4 e IPv6, quando o balanceamento é realizado apenas em direção ao servidor, onde a resposta do servidor real é enviada diretamente ao cliente;

1.1.19.48.4. Permitir a clonagem de pools, de forma que a solução envie uma cópia do tráfego para um pool adicional, como por exemplo um pool de IDSs ou Sniffers, para fins de análise de tráfego de rede ou mesmo para identificação de padrões de acesso não permitidos ou indicações de atividade maliciosas ou ataques de rede;

1.1.19.48.5. Possuir recursos para balancear servidores com qualquer hardware, sistema operacional e tipo de aplicação;

1.1.19.48.6. A solução deve possuir recurso de ativação de grupo prioritário, no qual o

administrador pode especificar a quantidade mínima de servidores que devem estar disponíveis em cada grupo e a prioridade dos grupos.

1.1.19.48.7. Caso o número de servidores disponíveis fique menor do que o estipulado pelo administrador, a solução deve automaticamente distribuir o tráfego para o próximo grupo com maior prioridade não afetando o serviço.

1.1.19.48.8. Caso o número de servidores disponíveis volte ao valor mínimo estipulado pelo administrador, a solução deve automaticamente retirar o grupo com menor prioridade de balanceamento, voltando ao estado original.

1.1.19.48.9. Possuir capacidade de abrir um número reduzido de conexões TCP com o servidor e inserir os HTTP requests gerado pelos clientes nestas conexões, reduzindo a necessidade de estabelecimento de conexões nos servidores e aumentando a performance do serviço;

1.1.19.48.10. Suportar os seguintes métodos de balanceamento:

1.1.19.48.10.1. Round Robin;

1.1.19.48.10.2. Least Connections;

1.1.19.48.10.3. Weighted Percentage (por peso);

1.1.19.48.10.4. Servidor ou equipamento com resposta mais rápida baseado no tráfego real;

1.1.19.48.10.5. Weighted Percentage dinâmico (baseado no número de conexões)

1.1.19.48.10.6. Dinâmico, baseado em parâmetros de um determinado servidor ou equipamento, coletados via SNMP ou WMI;

1.1.19.48.11. A solução deve permitir aplicar criptografia de cookies para a proteção dos cookies utilizados pela aplicação web;

1.1.19.48.12. Possuir recursos para balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência de sessão dos seguintes tipos:

1.1.19.48.12.1. Por cookie: inserção de um novo cookie na sessão;

1.1.19.48.12.2. Por cookie: utilização do valor do cookie da aplicação, sem adição de cookie;

1.1.19.48.12.3. Por endereço IP destino;

1.1.19.48.12.4. Por endereço IP origem;

1.1.19.48.12.5. Por sessão SSL;

1.1.19.48.12.6. Através da análise da URL acessada.;

1.1.19.48.12.7. Através da análise de qualquer parâmetro no header HTTP;

1.1.19.48.12.8. Através da análise do MS Terminal Services Session (MSRDP)
1.1.19.48.12.9. Através da análise do SIP Call ID ou Source IP;

1.1.19.48.12.10. Através da análise de qualquer informação da porção de dados (camada 7);

1.1.19.48.13. A solução deve utilizar Cache Array Routing Protocol (CARP) no algoritmo de HASH;

1.1.19.48.14. Deve suportar os seguintes métodos de monitoramento dos servidores reais:

1.1.19.48.14.1. ICMP;

1.1.19.48.14.2. Conexões TCP e UDP pela respectiva porta no servidor;

1.1.19.48.14.3. Devem existir monitores predefinidos para, no mínimo, os seguintes protocolos: ICMP, HTTP, HTTPS, Diameter, FTP, SASP, SMB, RADIUS, MSSQL,

NNTP, ORACLE, RPC, LDAP, IMAP, SMTP, POP3, SIP, Real Server, SOAP, SNMP e WMI;

1.1.19.48.15. Possuir recursos para balanceamento de carga de servidores SIP para VoIP (equipamento SIP PROXY);

1.1.19.48.16. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor físico:;

1.1.19.48.17. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor virtual;

1.1.19.48.18. Possuir recursos para limitar o número de sessões estabelecidas com cada grupo de servidores;

1.1.19.48.19. Realizar Network Address Translation (NAT);

1.1.19.48.20. Realizar Proteção contra Denial of Service (DoS);

1.1.19.48.21. Realizar Proteção contra Syn flood;

1.1.19.48.22. Realizar Limpeza de cabeçalho HTTP;

1.1.19.48.23. Deve permitir o controle da resposta ICMP por servidor virtual;

1.1.19.48.24. Possuir recursos para que a configuração seja baseada em perfis, permitindo uma fácil administração;

1.1.19.48.25. Possuir capacidade de geração e gestão de perfis hierarquizados, permitindo maior facilidade na administração de políticas similares;

1.1.19.48.26. Permitir a criação de Virtual Servers com endereço IPv4 e os servidores reais com endereços IPv6;

1.1.19.48.27. Possuir recursos para executar compressão de conteúdo HTTP, para reduzir a quantidade de informações enviadas ao cliente;

1.1.19.48.28. Definir qual tipo de compressão será habilitada (gzip1 a gzip9, deflate);

1.1.19.48.29. Possuir capacidade para definir compressão especificamente para certos tipos de objetos;

1.1.19.48.30. Permitir a utilização de memória RAM como cache de objetos HTTP, para responder às requisições dos usuários sem utilizar recursos dos servidores;

1.1.19.48.31. Permitir definir quais tipos de objeto serão armazenados em cache e quais nunca devem ser cacheados;

1.1.19.48.32. Garantir que o recurso de cache possa ajustar quanta memória será utilizada para armazenar objetos;

1.1.19.48.33. Suporte a otimização do protocolo TCP para ajustes a parâmetros das conexões clientes e servidor;

1.1.19.48.34. Deve possuir relatórios das aplicações, com pelos menos os seguintes gráficos:

1.1.19.48.34.1. Tempo de resposta da aplicação;

1.1.19.48.34.2. Latência ;

1.1.19.48.34.3. Conexões para conjunto de servidores, servidores individuais;

1.1.19.48.34.4. Por URL;

1.1.19.48.35. A ferramenta de relatórios deve possuir pelo menos os seguintes filtros para a geração dos gráficos:

1.1.19.48.35.1. Servidores virtuais

1.1.19.48.35.2. Servidores balanceados

1.1.19.48.35.3. URLs

1.1.19.48.35.4. Países de origem, baseados em geolocalização (GEOIP)

1.1.19.48.35.5. Dispositivos de origem do cliente (user agent)

1.1.19.48.36. Deve possuir framework unificado para configuração da aplicação

1.1.19.48.37. Quando licenciada, a solução deve ter a capacidade de realizar cache transparente das respostas DNS;

1.1.19.48.38. A Solução deve ter suporte a sFlow;

1.1.19.48.39. A solução deve possuir múltiplos domínios de roteamento em IPv4 e IPv6;
1.1.19.48.40. A solução deve permitir que cada domínio de roteamento utilize BGP, OSPF e RIP em IPv4 e IPv6;

1.1.19.48.41. A solução deve suportar Equal Cost Multipath (ECMP);

1.1.19.48.42. A solução deve realizar Bidirectional Forward Detection (BFD);

1.1.19.48.43. A solução deve ter suporte a Stream Control Transmission Protocol (SCTP);

1.1.19.48.44. Deve ter suporte a Transport Layer Security (TLS) Server Name Indication (SNI);
1.1.19.48.45. A solução deve possuir monitor HTTP/HTTPS com autenticação NTLM embutida, que permita verificar se o HTTP/HTTPS está operando assim como a plataforma de autenticação;

1.1.19.48.46. A solução deve ter suporte a TLS 1.2, SHA 2 Cipher e SHA256 hash;

1.1.19.48.47. A solução deve ter suporte a criptografia Perfect Forward Secrecy não apenas para troca de chaves RSA.

1.1.19.48.48. A solução deve ser capaz de colocar em fila as requisições TCP que excedam a capacidade de conexões do grupo de servidores ou de um servidor. A solução não deverá descartar as conexões que excedam o número de conexões do servidor ou do grupo de servidores:

1.1.19.48.49. Deve ser possível configurar o tamanho máximo da fila;

1.1.19.48.50. Deve ser possível configurar o tempo máximo de permanência na fila;

1.1.19.48.51. A solução deve realizar Controle de Banda Estático para grupos de aplicações e rede;

1.1.19.48.52. A solução deve realizar Controle de Banda Dinâmico por aplicação e usuário;
1.1.19.48.53. A solução deve realizar Controle de Banda baseado em domínio de roteamento;
1.1.19.48.54. Permitir tráfego por parâmetros de QoS (Quality of Service) ou rate-shaping, com pelo menos 2 (duas) filas para priorização de tráfego baseada na camada de aplicação;

1.1.19.48.55. Através dessa priorização de tráfego e restrição de largura de banda deverá ser possível permitir um melhor nível de serviço para clientes preferenciais em detrimento dos demais clientes.

1.1.19.48.56. A solução deve permitir a priorização de tráfego de entrada para determinadas aplicações.

1.1.19.48.57. A solução deve permitir a criação de túneis IP por domíno de roteamento utilizando GRE, IPIP, EtherIP, PPP;

1.1.19.48.58. A solução deve permitir a criação de túneis IP transparente utilizando GRE e IPIP;
1.1.19.48.59. Fornecer recursos para o uso de servidores (reals) no mesmo Virtual Server;

1.1.19.48.60. Possuir suporte ao protocolo SPDY e HTTP 2.0;

1.1.19.48.61. O equipamento deve possuir suporte ao espelhamento de conexões FTP, Telnet, HTTP, UDP, SSL.

1.1.19.48.62. O equipamento deverá permitir a sincronização das configurações:

1.1.19.48.62.1. De forma automática; e

1.1.19.48.62.2. Manualmente, forçando a sincronização apenas no momento desejado;
1.1.19.48.63. Permitir que regras customizadas em linguagem aberta possam ser utilizadas para

customizar a distribuição dinâmica de tráfego e aumentar a proteção contra ataques;

1.1.19.48.64. A solução deve possuir linguagem de programação open-source que permita a manipulação do tráfego de entrada e saída, viabilizando assim a alteração de parâmetros no cabeçalho e no corpo das mensagens.

1.1.19.48.65. Essa linguagem de programação deve permitir a importação de pacotes, garantindo assim que a agilidade e flexibilidade no compartilhamento dos scripts.

1.1.19.48.66. Permitir a criação de políticas através de interface gráfica web para manipulação de tráfego através de lógica para pelo menos os seguintes operadores:

1.1.19.48.66.1. GEOIP, http-basic-auth, http-cookie, http-header, http-host, http-method, http-referer, http-set-cookie, http-status, http-uri e http-version

1.1.19.48.67. Deve ser possível tomar as seguintes ações através dessas políticas:

1.1.19.48.67.1. Bloqueio de tráfego

1.1.19.48.67.2. Reescrita e manipulação de URL 1.1.19.48.67.3. Registro de tráfego (log)

1.1.19.48.67.4. Adição de informação no cabeçalho HTTP

1.1.19.48.67.5. Redirecionamento do tráfego para um membro específico

1.1.19.48.67.6. Selecionar uma política específica para Aplicação Web

1.1.19.48.68. A solução deverá ser capaz de fazer log de todas as sessões, onde os registros deverão conter:

1.1.19.48.68.1. Endereço IP de origem;

1.1.19.48.68.2. Porta TCP ou UDP de origem;

1.1.19.48.68.3. Endereço IP de destino;

1.1.19.48.68.4. Porta TCP ou UDP de destino;

1.1.19.48.68.5. Protocolo de camada 4 (TCP ou UDP);

1.1.19.48.68.6. Data e hora da mensagem;

1.1.19.48.68.7. URL acessada;

1.1.19.48.69. A solução deve possuir políticas de uso de senhas administrativas tais como: nível de complexidade, período de validade e travamento de conta devido a erros múltiplos de login de forma nativa ou no mínimo integrado a uma base Active Directory.

1.1.19.48.70. A solução deve suportar controle de versão da política de configuração de forma a permitir fazer roll back de políticas aplicadas.

1.1.19.49. Funcionalidades para alta disponibilidade entre ambientes de Datacenter

1.1.19.49.1. Fornecer recurso de agregação de portas baseado no protocolo LACP;

1.1.19.49.2. Deve possuir suporte a LACP em modo passivo e ativo;

1.1.19.49.3. Fornecer recurso para suportar até 8 portas em um mesmo conjunto agregado;
1.1.19.49.4. Deve possuir suporte a Spanning-Tree(802.1D), Fast Spanning-Tree (802.1w, 802.1t) e Multi Spanning-Tree (802.1s);

1.1.19.49.5. Fornecer recurso para o transporte de múltiplas VLAN por uma única porta (ou por um conjunto agregado de portas) utilizando o protocolo 802.1q;

1.1.19.49.6. Possuir suporte a IPv6;

1.1.19.49.7. A solução deve suportar múltiplas tabelas de rotas independentes;

1.1.19.49.8. A solução deve possuir suporte a múltiplos domínios de roteamento em IPv4 e IPv6;

1.1.19.49.9. Possuir ferramenta online web gratuita na qual seja possível carregar as configurações e receber diagnóstico da solução com informações sobre atualizações, melhores práticas, estado da solução e informações preventivas.

1.1.19.49.10. A solução deve operar em, no mínimo, a seguintes formas:

1.1.19.49.10.1. DNS autoritativo;

1.1.19.49.10.2. DNS secundário;

1.1.19.49.10.3. DNS resolver;

1.1.19.49.10.4. DNS cache;

1.1.19.49.10.5. Balanceamento de DNS servers;

1.1.19.49.10.6. DNSSec;

1.1.19.49.11. A solução deve ser capaz de realizar transferência de zonas para múltiplos servidores DNS Primários responsáveis por diferentes zonas.

1.1.19.49.12. Deve possuir funcionalidade de DNS cache, realizando cache transparente, caching resolver e validação de caching resolver.

1.1.19.49.13. Capacidade de uso de chave criptográfica TSIG para comunicação segura entre servidores DNS, obedecendo no mínimo os padrões: HMAC MD5, HMAC SHA-1 ou HMAC SHA-256;

1.1.19.49.14. A solução deve realizar o offload dos servidores de DNS, funcionando como o DNS secundário;

1.1.19.49.15. A solução deve servir as respostas as requisições onde o DNS é o autoritativo a partir da memória RAM;

1.1.19.49.16. A solução deve possuir proteções contra ataques DNS, no mínimo:

1.1.19.49.16.1. Inspeção de protocolo;

1.1.19.49.16.2. Validação de protocolo;

1.1.19.49.16.3. UDP flood;

1.1.19.49.16.4. Pacotes malformados;

1.1.19.49.16.5. Ataque teardrop;

1.1.19.49.16.6. Ataque ICMP;

1.1.19.49.17. Permitir que regras customizadas em linguagem aberta possam ser utilizadas para customizar a distribuição dinâmica de tráfego e aumentar a proteção contra ataques;

1.1.19.49.18. A solução deve ser capaz de realizar balanceamento dos servidores DNS;
1.1.19.49.19. A solução deve ser capaz de realizar filtragem de pacotes;

1.1.19.49.20. A solução deve prover segurança do protocolo DNS, protegendo contra ataques de negação de serviço, NXDOMAIN e reflexão de DNS.

1.1.19.49.21. A solução deve prover segurança do protocolo DNS, protegendo contra ataques de Cache Poisoning.

1.1.19.49.22. A solução deve realizar stateful inspection;

1.1.19.49.23. A solução deve possuir base de Geolocalização IP;

1.1.19.49.24. A solução deve implementar DNS64;

1.1.19.49.25. A solução deve suportar pelo menos os seguintes tipos de requisição DNS: SOA, A, AAAA, CNAME, DNAME, HINFO, MX, NS, PTR, SRV, TXT

1.1.19.49.26. Deve ser capaz de gerar estatísticas sobre consultas de DNS por: Aplicação, nome da query, tipo da query, endereço IP do cliente;

1.1.19.49.27. Deve ser possível configurar a solução de modo inline a estrutura de DNS existente e transparente sem requerer grandes mudanças na infraestrutura;

1.1.19.49.28. Deve prover as respostas a queries DNS da própria RAM CACHE

1.1.19.49.29. A solução deve ser capaz de realizar IP Anycast;

1.1.19.49.30. A solução deve ser capaz de realizar DNSSec, independente da estrutura dos servidores DNS em uso;

1.1.19.49.31. A solução de alta disponibilidade não deve depender de BGP ou outro protocolo de roteamento;

1.1.19.49.32. A solução de alta disponibilidade será realizada baseada em respostas a requisições DNS. A resposta a requisições DNS devem conter apenas endereços que estejam disponíveis no momento, e balanceadas por usuário, de acordo com as políticas definidas;

1.1.19.49.33. A solução deverá aceitar resolução de nomes baseada em topologia, onde requisições de DNS são respondidas baseado no país, continente, ou endereço IP de onde veio a requisição;

1.1.19.49.34. Deve ser possível ajustar quantos endereços são enviados em uma única resposta;

1.1.19.49.35. Suporte a monitoração de estado de saúde de servidores, serviços e links de conexão a provedor de serviço, garantindo a disponibilidade do serviço oferecido entre datacenters;

1.1.19.49.36. Deve possuir suporte a monitoração de pelo menos 15 diferentes aplicações, incluindo SAP, Oracle, mySQL e LDAP.

1.1.19.49.37. Suportar pelo menos os seguintes algoritmos de balanceamento global:

1.1.19.49.37.1. Round Robin;

1.1.19.49.37.2. Global Availability;

1.1.19.49.37.3. Ratio;

1.1.19.49.37.4. LDNS Persist;

1.1.19.49.37.5. Geografia;

1.1.19.49.37.6. Disponibilidade da Aplicação;

1.1.19.49.37.7. Capacidade do Virtual Server;

1.1.19.49.37.8. Least Connections;

1.1.19.49.37.9. Pacotes por segundo;

1.1.19.49.37.10. Round trip time;

1.1.19.49.37.11. Hops;

1.1.19.49.37.12. Packet Completion Rate;

1.1.19.49.37.13. QoS definido pelo usuário;

1.1.19.49.37.14. Kilobytes per Second;

1.1.19.49.38. Implementar persistência da conexão do usuário entre aplicações ou data centers;

1.1.19.49.39. A solução deverá suportar o controle de grupos de aplicações, e permitir que um usuário seja redirecionado para outro datacenter quando houver falha em qualquer das aplicações de um mesmo grupo;

1.1.19.49.40. A solução deverá permitir que as políticas sejam configuradas individualmente por aplicação sendo balanceada;

1.1.19.49.41. A solução deverá permitir que a contingência seja automática, mas que o retorno seja manual;

1.1.19.49.42. A solução deve ser capaz de lidar com clientes IPv6 quando o site atende apenas com IPv4 (requests AAAA ou A6);

1.1.19.49.43. Possuir suporte a IPv6 no balanceamento global entre datacenters.

1.1.19.49.44. Ter capacidade de tratar informações das camadas L4-L7 (FTP, SMTP, URL, HTTP Header, TCP e UDP) para a tomada de decisão de encaminhamento a servidor real, em IPv4 e IPv6.

1.1.19.49.45. Deverá possuir a funcionalidade de resposta rápida a queries DNS. permitindo respostas mais rápidas para zonas que seja autoritativo.

1.1.19.49.46. A solução deve possuir suporte a Response Policy Zones (RPZ), mecanismo de firewall usado por DNS recursivo para permitir o tratamento customizado da resolução de nomes. Portanto a solução deve ser capaz de filtrar queries DNS para domínios considerados maliciosos e retornar respostas customizadas.

1.1.19.49.47. A solução deve possuir linguagem de programação open-source que permita a manipulação do tráfego de entrada e saída, viabilizando assim a alteração de parâmetros no cabeçalho e no corpo das mensagens.

1.1.19.49.48. Essa linguagem de programação deve permitir a importação de pacotes, garantindo assim que a agilidade e flexibilidade no compartilhamento dos scripts.

1.1.19.49.49. Deve estender a funcionalidade de programabilidade com Node.js, provendo um ambiente para rodar JavaScript independente de web browser.

1.1.20. ITEM 20 – FIREWALL DE APLICAÇÃO WEB – WAF – DATACENTER TIPO I

1.1.20.1. Os appliances físicos devem ser novos e de primeiro uso;

1.1.20.2. Os equipamentos devem ser fornecidos em modo appliance, com conjunto de hardware e software dedicados, não podendo ser servidor de uso genérico, e que atendam todas as funcionalidades descritas neste Termo de Referência;

1.1.20.3. Devem ser novos, sem uso prévio e entregues em perfeito estado de funcionamento. Não devem ser remanufaturados, recondicionados ou possuir reparos de qualquer espécie;

1.1.20.4. Não serão aceitos equipamentos ou softwares que constem em anúncio ou lista do tipo end-of-sale, end-of-support ou end-of-life do fabricante, ou seja, produtos que serão descontinuados, perderão suporte e garantia oficiais do fabricante;

1.1.20.5. Deverão ser fornecidos todos os cabos, suportes (se necessários, "gavetas", "braços" e "trilhos"), incluindo todos os cabos de ligação lógica e elétrica necessários à instalação e perfeito

funcionamento do equipamento no rack;

1.1.20.6. Dispor de fonte de alimentação redundante com tensão de entrada de 110V a 220V AC automática e frequência de 60Hz;

1.1.20.7. Possuir sistema operacional customizado especificamente para funções de Web Application Firewall, não podendo ser entregue appliance do tipo NGFW;

1.1.20.8. A solução deve ser licenciada para uso perpétuo. As funcionalidades da solução devem permanecer ativas após o período de garantia mesmo que desatualizadas e com todas as atualizações e assinaturas que forem disponibilizadas até data final do período que foram aplicadas ou instaladas na solução;

1.1.20.9. Possuir, no mínimo, 04 (quatro) interfaces de 10GE SFP+. Serão aceitas interfaces de maior capacidade, desde que possibilitem ser transformados em 10 GE (incluindo os cabos “breakout” de no mínimo 3 metros);

1.1.20.10. Possuir, pelo menos, 04 (quatro) interfaces 10G/1G RJ-45;

1.1.20.11. Possuir 01 interfaces 1GE, incluso interfaces de gerência com conectores padrão RJ45;

1.1.20.12. Todas as interfaces fornecidas devem estar licenciadas e habilitadas para uso imediato;

1.1.20.13. Deve possuir capacidade de inspecionar, no mínimo, 16 (dezesseis) Gbps de tráfego web em camada 7;

1.1.20.14. Suportar no mínimo 9.000 (nove mil) transações por segundo (TPS) SSL utilizando curva elíptica (ECDHE) com chaves RSA 2048 bits;

1.1.20.15. Suportar 18.000.000 (dezoito milhões) de conexões concorrentes em camada 4;

1.1.20.16. Possuir no mínimo compressão de 14.000 Mbps em tráfego HTTP/HTTPS;

1.1.20.17. Recursos de agregação de portas baseado no protocolo LACP, segundo o padrão IEEE 802.3ad;

1.1.20.18. Memória RAM mínima de 32 GB;

1.1.20.19. Disco rígido com capacidade de armazenamento interno e retenção de logs para análise com capacidade mínima de 420GB;

1.1.20.20. Deve vir acompanhado de todas as licenças de software ou hardware necessárias para atendimento das funcionalidades exigidas neste caderno de especificações técnicas;

1.1.20.21. Garantir que na aceleração de SSL, tanto a troca de chaves quanto a criptografia dos dados seja realizada com aceleração em hardware, para não onerar o sistema;

1.1.20.22. Deve permitir a configuração da solução em alta disponibilidade, permitindo o funcionamento em cluster do tipo ativo-passivo e ativo-ativo;

1.1.20.23. A solução deve suportar mais do que dois elementos no cluster para sincronização de configuração de forma nativa a fim de permitir escalabilidade no futuro;

1.1.20.24. Implementar a sincronização entre os equipamentos redundantes, assegurando que não haverá "downtime" e queda de sessões em caso de falha de uma das unidades;

1.1.20.25. Possuir recurso para o transporte de múltiplas VLANs por uma única porta (ou por um conjunto agregado de portas) utilizando o protocolo 802.1q;

1.1.20.26. Deve suportar, no mínimo, 1000 VLANs simultaneamente;

1.1.20.27. Analisar e proteger tráfego HTTP/1.0, HTTP/1.1, HTTP/2.0 e/ou HTTP/3;

1.1.20.28. Possuir suporte a IPv6;

1.1.20.29. A solução deve permitir o encapsulamento, em camada 3, do tráfego entre o balanceador e o servidor para tráfego IPv4 e IPv6, quando o balanceamento é realizado apenas

em direção ao servidor, onde a resposta do servidor real é enviada diretamente ao cliente;

1.1.20.30. Possuir suporte à funcionalidade de VXLAN para integração com o ambiente de virtualização (Software Defined Network);

1.1.20.31. Assinar cookies digitalmente e editar endereços de URL (“URL Rewriting”);

1.1.20.32. Os usuários de gerência deverão poder ser autenticados em bases remotas. No mínimo RADIUS, LDAP e TACACS+ deverão ser suportados;

1.1.20.33. Deverá possuir uma funcionalidade de criação automática de políticas, para proteção DDOS e ataques zero-day onde a política de segurança é criada e atualizada automaticamente baseando-se no tráfego real observado à aplicação;

1.1.20.34. Restringir métodos HTTP/ HTTPS permitidos, tipos ou versões de protocolos, tipos de caracteres e versões utilizadas de cookies;

1.1.20.35. Permitir as seguintes opções de implementação:

1.1.20.36. Monitoramento (sem bloqueio);

1.1.20.37. Proxy (reverso e transparente);

1.1.20.38. Permitir que novas políticas fiquem apenas monitorando o tráfego, sem bloqueá-lo, indicando caso aconteça algum evento;

1.1.20.39. Remover as mensagens de erro do conteúdo que será enviado aos usuários;

1.1.20.40. Proteger contra-ataques automatizados, incluindo bots e web scraping, identificando comportamento não humano, navegadores operados por scripts ou qualquer outra forma que não operados por humanos;

1.1.20.41. Possuir firewall XML integrado com suporte a filtro e validação de funções XML específicas da aplicação;

1.1.20.42. A solução deve suportar e fazer a proteção do tráfego de protocolo WebSocket;

1.1.20.43. Permitir a utilização de modelo positivo de segurança para proteger contra ataques às aplicações HTTP e HTTPS, além de proteção contra- ataques conhecidos aos protocolos HTTP e HTTPS;

1.1.20.44. Criação de políticas automáticas que bloqueiam o endereço IP que realizar violações;

1.1.20.45. Possuir mecanismo de aprendizado automatizado capaz de identificar todos os conteúdos das aplicações, incluindo URLs, parâmetros URLs, campos de formulários, o que se espera de

cada campo (tipo de dado, tamanho de caracteres, se é um campo obrigatório), cookies, ações SOAP e elementos XML. Identificar e criar perfil de utilização dos aplicativos, inclusive desenvolvidos em Javascript, CGI, ASP e PHP;

1.1.20.46. Deve possuir tecnologia para mitigação de DDoS em camada 7 baseado em análise comportamental, usando o aprendizado;

1.1.20.47. A solução deve possuir a capacidade de capturar tráfego no formato TCP Dump relativos a ataques DoS L7, Web Scraping e força bruta permitindo uma análise mais aprofundada por parte do administrador;

1.1.20.48. Detectar ataques de força bruta por meio dos seguintes métodos:

1.1.20.49. Aumento do tempo de resposta da aplicação monitorada ou bloqueio temporário do atacante;

1.1.20.50. Quantidade de transações por segundo (TPS), monitorando a quantidade de transações por segundo por endereço IP;

1.1.20.51. Permitir a criação de políticas diferenciadas por aplicação e por URL, onde cada aplicação e URL poderão ter políticas totalmente diferentes;

1.1.20.52. Apresentar proteção contra-ataques, como:

1.1.20.53. Brute Force Login;

1.1.20.54. Buffer Overflow;

1.1.20.55. Cookie Injection;

1.1.20.56. Cookie Poisoning;

1.1.20.57. Cross Site Request Forgery (CSRF);

1.1.20.58. Cross Site Scripting (XSS);

1.1.20.59. Server Side Request Forgery (SSRF);

1.1.20.60. Directory Traversal;

1.1.20.61. Forceful Browsing;

1.1.20.62. HTTP Denial of Service;

1.1.20.63. HTTP hidden field manipulation;

1.1.20.64. HTTP request smuggling;

1.1.20.65. HTTP Response Splitting;

1.1.20.66. Malicious Robots;

1.1.20.67. Parameter Tampering;

1.1.20.68. Remote File Inclusion Attacks;

1.1.20.69. Sensitive Data Leakage (Social Security Numbers, Cardholder Data, PII, HPI);

1.1.20.70. Session Hijacking;

1.1.20.71. SQL Injection;

1.1.20.72. Web Scraping;

1.1.20.73. Web server software and operating system attacks;

1.1.20.74. Web Services (XML) attacks;

1.1.20.75. Deve permitir que possa ser especificado na política os tipos de arquivos que serão bloqueados (File Types);

1.1.20.76. A solução deve permitir a inspeção de upload de arquivos para os servidores de aplicação, ou enviar para inspeção através do protocolo ICAP;

1.1.20.77. Deve encriptar dados e credenciais na camada de aplicação, sem ter a necessidade de atualizar a aplicação. Essas informações devem ser encriptadas para proteger o login e as credenciais dos usuários e com isso os dados da aplicação;

1.1.20.78. Deve proteger informações sensíveis e confidenciais da interceptação por terceiros, através da criptografia de dados quando ainda no browser do usuário. Deve proteger esses dados criptografados de malwares e keyloggers;

1.1.20.79. Deve ofuscar o nome de um parâmetro sensível da aplicação em caracteres randômicos. Esse nome de parâmetro deve ser mudado constantemente pela ferramenta para dificultar ataques direcionados;

1.1.20.80. A solução deve fornecer relatórios consolidados de ataques com pelo menos os seguintes dados:

1.1.20.81. Resumo geral com as políticas ativas, anomalias e estatísticas de tráfego, Ataques DoS, Ataques de Força Bruta, Ataques de Robôs, Violações, URL, Endereços IP, Países, Severidade;

1.1.20.82. Deverá permitir o agendamento de relatórios a serem entregues por email;

1.1.20.83. Emitir os seguintes relatórios gráficos por:

1.1.20.84. Política de segurança;

1.1.20.85. Tipos de ataques;

1.1.20.86. Violações;

1.1.20.87. URL que foram atacadas;

1.1.20.88. Endereços IP de origem;

1.1.20.89. Localização geográfica dos endereços IPs de origem;

1.1.20.90. Severidade;

1.1.20.91. Código de resposta;

1.1.20.92. Métodos;

1.1.20.93. Protocolos;

1.1.20.94. Sessão;

1.1.20.95. A solução deve ser capaz de proteger GraphQL APIs com pelos menos os seguintes parâmetros: tamanho total, tamanho de cada parâmetro

1.1.20.96. A solução deve ser capaz de proteger GraphQL APIs limitando a quantidade de queries dentro de uma requisição HTTP

1.1.20.97. A solução deve ser capaz de proteger APIs baseadas em OpenAPI 2.0

1.1.20.98. A solução deve ser capaz de proteger APIs baseadas em OpenAPI 3.0

1.1.20.99. A solução deve suportar a criação de políticas de proteção com base no modelo OWASP, onde pelo menos devem ser aplicadas políticas de proteção contra o TOP 10 OWASP

1.1.20.100. A solução deve emitir relatório com análise cada política de proteção comparado com o TOP 10 OWASP.

1.1.20.101. A solução deverá possuir as seguintes formas de detecção de ataques DoS na camada de aplicação:

1.1.20.102. Número de requisições por segundo enviados a uma URL específica;

1.1.20.103. Número de requisições por segundo enviados de um IP específico;

1.1.20.104. Detecção através de código executado no cliente com o objetivo de detectar interação humana ou comportamento de robôs (bots);

1.1.20.105. Número máximo de transações por segundo (TPS) de um determinado IP;

1.1.20.106. Aumento de um determinado percentual do número de transações por segundo (TPS);

1.1.20.107. Aumento do stress do servidor de aplicação;

1.1.20.108.

1.1.20.109. Funcionalidades de Balanceamento de Carga

1.1.20.110. Deve suportar todas as aplicações comuns de um Switch Layer 7, como:

1.1.20.111. Server Load-Balancing;

1.1.20.112. Firewall Load-Balancing;

1.1.20.113. Proxy Load-Balancing;

1.1.20.114. Deve suportar balanceamento apenas em direção ao servidor, onde a resposta do servidor real é enviada diretamente ao cliente;

1.1.20.115. Deve permitir o encapsulamento, em camada 3, do tráfego entre a solução e o servidor para tráfego IPv4 e IPv6, quando o balanceamento é realizado apenas em direção ao servidor, onde a resposta do servidor real é enviada diretamente ao cliente;

1.1.20.116. Permitir a clonagem de pools, de forma que a solução envie uma cópia do tráfego para um pool adicional, como por exemplo um pool de IDSs ou Sniffers, para fins de análise de tráfego de rede ou mesmo para identificação de padrões de acesso não permitidos ou indicações de atividade maliciosas ou ataques de rede;

1.1.20.117. Possuir recursos para balancear servidores com qualquer hardware, sistema operacional e tipo de aplicação;

1.1.20.118. A solução deve possuir recurso de ativação de grupo prioritário, no qual o administrador pode especificar a quantidade mínima de servidores que devem estar disponíveis em cada grupo e a prioridade dos grupos.

1.1.20.119. Caso o número de servidores disponíveis fique menor do que o estipulado pelo administrador, a solução deve automaticamente distribuir o tráfego para o próximo grupo com maior prioridade não afetando o serviço.

1.1.20.120. Caso o número de servidores disponíveis volte ao valor mínimo estipulado pelo administrador, a solução deve automaticamente retirar o grupo com menor prioridade de balanceamento, voltando ao estado original.

1.1.20.121. Possuir capacidade de abrir um número reduzido de conexões TCP com o servidor e inserir os HTTP requests gerado pelos clientes nestas conexões, reduzindo a necessidade de estabelecimento de conexões nos servidores e aumentando a performance do serviço;

1.1.20.122. Suportar os seguintes métodos de balanceamento:

1.1.20.123. Round Robin;

1.1.20.124. Least Connections;

1.1.20.125. Weighted Percentage (por peso);

1.1.20.126. Servidor ou equipamento com resposta mais rápida baseado no tráfego real;

1.1.20.127. Weighted Percentage dinâmico (baseado no número de conexões)

1.1.20.128. Dinâmico, baseado em parâmetros de um determinado servidor ou equipamento, coletados via SNMP ou WMI;

1.1.20.129. A solução deve permitir aplicar criptografia de cookies para a poteção dos cookies utilizados pela aplicação web;

1.1.20.130. Possuir recursos para balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência de sessão dos seguintes tipos:

1.1.20.131. Por cookie: inserção de um novo cookie na sessão;

1.1.20.132. Por cookie: utilização do valor do cookie da aplicação, sem adição de cookie;
1.1.20.133. Por endereço IP destino;

1.1.20.134. Por endereço IP origem;

1.1.20.135. Por sessão SSL;

1.1.20.136. Através da análise da URL acessada.;

1.1.20.137. Através da análise de qualquer parâmetro no header HTTP;

1.1.20.138. Através da análise do MS Terminal Services Session (MSRDP)

1.1.20.139. Através da análise do SIP Call ID ou Source IP;

1.1.20.140. Através da análise de qualquer informação da porção de dados (camada 7);

1.1.20.141. A solução deve utilizar Cache Array Routing Protocol (CARP) no algoritmo de HASH;

1.1.20.142. Deve suportar os seguintes métodos de monitoramento dos servidores reais:

1.1.20.143. ICMP;

1.1.20.144. Conexões TCP e UDP pela respectiva porta no servidor;

1.1.20.145. Devem existir monitores predefinidos para, no mínimo, os seguintes protocolos: ICMP, HTTP, HTTPS, Diameter, FTP, SASP, SMB, RADIUS, MSSQL, NNTP, ORACLE, RPC, LDAP, IMAP, SMTP, POP3, SIP, Real Server, SOAP, SNMP e WMI;

1.1.20.146. Possuir recursos para balanceamento de carga de servidores SIP para VoIP (equipamento SIP PROXY);

1.1.20.147. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor físico:

1.1.20.148. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor virtual;

1.1.20.149. Possuir recursos para limitar o número de sessões estabelecidas com cada grupo de

servidores;

1.1.20.150. Realizar Network Address Translation (NAT);

1.1.20.151. Realizar Proteção contra Denial of Service (DoS);

1.1.20.152. Realizar Proteção contra Syn flood;

1.1.20.153. Realizar Limpeza de cabeçalho HTTP;

1.1.20.154. Deve permitir o controle da resposta ICMP por servidor virtual;

1.1.20.155. Possuir recursos para que a configuração seja baseada em perfis, permitindo uma fácil administração;

1.1.20.156. Possuir capacidade de geração e gestão de perfis hierarquizados, permitindo maior facilidade na administração de políticas similares;

1.1.20.157. Permitir a criação de Virtual Servers com endereço IPv4 e os servidores reais com endereços IPv6;

1.1.20.158. Possuir recursos para executar compressão de conteúdo HTTP, para reduzir a quantidade de informações enviadas ao cliente;

1.1.20.159. Definir qual tipo de compressão será habilitada (gzip1 a gzip9, deflate);

1.1.20.160. Possuir capacidade para definir compressão especificamente para certos tipos de objetos;

1.1.20.161. Permitir a utilização de memória RAM como cache de objetos HTTP, para responder às

requisições dos usuários sem utilizar recursos dos servidores;

1.1.20.162. Permitir definir quais tipos de objeto serão armazenados em cache e quais nunca devem ser cacheados;

1.1.20.163. Garantir que o recurso de cache possa ajustar quanta memória será utilizada para armazenar objetos;

1.1.20.164. Suporte a otimização do protocolo TCP para ajustes a parâmetros das conexões clientes e servidor;

1.1.20.165. Deve possuir relatórios das aplicações, com pelos menos os seguintes gráficos:
1.1.20.166. Tempo de resposta da aplicação;

1.1.20.167. Latência ;

1.1.20.168. Conexões para conjunto de servidores, servidores individuais;

1.1.20.169. Por URL;

1.1.20.170. A ferramenta de relatórios deve possuir pelo menos os seguintes filtros para a geração dos gráficos:

1.1.20.171. Servidores virtuais

1.1.20.172. Servidores balanceados

1.1.20.173. URLs

1.1.20.174. Países de origem, baseados em geolocalização (GEOIP)

1.1.20.175. Dispositivos de origem do cliente (user agent)

1.1.20.176. Deve possuir framework unificado para configuração da aplicação

1.1.20.177. Quando licenciada, a solução deve ter a capacidade de realizar cache transparente das respostas DNS;

1.1.20.178. A Solução deve ter suporte a sFlow;

1.1.20.179. A solução deve possuir múltiplos domínios de roteamento em IPv4 e IPv6;

1.1.20.180. A solução deve permitir que cada domínio de roteamento utilize BGP, OSPF e RIP em IPv4 e IPv6;

1.1.20.181. A solução deve suportar Equal Cost Multipath (ECMP);

1.1.20.182. A solução deve realizar Bidirectional Forward Detection (BFD);

1.1.20.183. A solução deve ter suporte a Stream Control Transmission Protocol (SCTP);

1.1.20.184. Deve ter suporte a Transport Layer Security (TLS) Server Name Indication (SNI);

1.1.20.185. A solução deve possuir monitor HTTP/HTTPS com autenticação NTLM embutida, que permita verificar se o HTTP/HTTPS está operando assim como a plataforma de autenticação;

1.1.20.186. A solução deve ter suporte a TLS 1.2, SHA 2 Cipher e SHA256 hash;

1.1.20.187. A solução deve ter suporte a criptografia Perfect Forward Secrecy não apenas para troca de chaves RSA.

1.1.20.188. A solução deve ser capaz de colocar em fila as requisições TCP que excedam a capacidade de conexões do grupo de servidores ou de um servidor. A solução não deverá descartar as conexões que excedam o número de conexões do servidor ou do grupo de servidores:

1.1.20.189. Deve ser possível configurar o tamanho máximo da fila;

1.1.20.190. Deve ser possível configurar o tempo máximo de permanência na fila;

1.1.20.191. A solução deve realizar Controle de Banda Estático para grupos de aplicações e rede;
1.1.20.192. A solução deve realizar Controle de Banda Dinâmico por aplicação e usuário;
1.1.20.193. A solução deve realizar Controle de Banda baseado em domínio de roteamento;

1.1.20.194. Permitir tráfego por parâmetros de QoS (Quality of Service) ou rate-shaping, com pelo menos 2 (duas) filas para priorização de tráfego baseada na camada de aplicação;

1.1.20.195. Através dessa priorização de tráfego e restrição de largura de banda deverá ser possível permitir um melhor nível de serviço para clientes preferenciais em detrimento dos demais clientes.

1.1.20.196. A solução deve permitir a priorização de tráfego de entrada para determinadas aplicações.

1.1.20.197. A solução deve permitir a criação de túneis IP por domíno de roteamento utilizando GRE,

IPIP, EtherIP, PPP;

1.1.20.198. A solução deve permitir a criação de túneis IP transparente utilizando GRE e IPIP;
1.1.20.199. Fornecer recursos para o uso de servidores (reals) no mesmo Virtual Server;

1.1.20.200. Possuir suporte ao protocolo SPDY e HTTP 2.0;

1.1.20.201. O equipamento deve possuir suporte ao espelhamento de conexões FTP, Telnet, HTTP, UDP, SSL.

1.1.20.202. O equipamento deverá permitir a sincronização das configurações:

1.1.20.203. De forma automática; e

1.1.20.204. Manualmente, forçando a sincronização apenas no momento desejado;

1.1.20.205. Permitir que regras customizadas em linguagem aberta possam ser utilizadas para customizar a distribuição dinâmica de tráfego e aumentar a proteção contra ataques;

1.1.20.206. A solução deve possuir linguagem de programação open-source que permita a manipulação do tráfego de entrada e saída, viabilizando assim a alteração de parâmetros no cabeçalho e no corpo das mensagens.

1.1.20.207. Essa linguagem de programação deve permitir a importação de pacotes, garantindo assim que a agilidade e flexibilidade no compartilhamento dos scripts.

1.1.20.208. Permitir a criação de políticas através de interface gráfica web para manipulação de tráfego através de lógica para pelo menos os seguintes operadores:

1.1.20.209. GEOIP, http-basic-auth, http-cookie, http-header, http-host, http-method, http-referer, http- set-cookie, http-status, http-uri e http-version

1.1.20.210. Deve ser possível tomar as seguintes ações através dessas políticas:

1.1.20.211. Bloqueio de tráfego

1.1.20.212. Reescrita e manipulação de URL

1.1.20.213. Registro de tráfego (log)

1.1.20.214. Adição de informação no cabeçalho HTTP

1.1.20.215. Redirecionamento do tráfego para um membro específico

1.1.20.216. Selecionar uma política específica para Aplicação Web

1.1.20.217. A solução deverá ser capaz de fazer log de todas as sessões, onde os registros deverão conter:

1.1.20.218. Endereço IP de origem;

1.1.20.219. Porta TCP ou UDP de origem;

1.1.20.220. Endereço IP de destino;

1.1.20.221. Porta TCP ou UDP de destino;

1.1.20.222. Protocolo de camada 4 (TCP ou UDP);

1.1.20.223. Data e hora da mensagem;

1.1.20.224. URL acessada;

1.1.20.225. A solução deve possuir políticas de uso de senhas administrativas tais como: nível de complexidade, período de validade e travamento de conta devido a erros múltiplos de login de forma nativa ou no mínimo integrado a uma base Active Directory.

1.1.20.226. A solução deve suportar controle de versão da política de configuração de forma a permitir fazer roll back de políticas aplicadas.

1.1.20.227. Funcionalidades para alta disponibilidade entre ambientes de Datacenter

1.1.20.228. Fornecer recurso de agregação de portas baseado no protocolo LACP;

1.1.20.229. Deve possuir suporte a LACP em modo passivo e ativo;

1.1.20.230. Fornecer recurso para suportar até 8 portas em um mesmo conjunto agregado;
1.1.20.231. Deve possuir suporte a Spanning-Tree(802.1D), Fast Spanning-Tree (802.1w, 802.1t) e

Multi Spanning-Tree (802.1s);

Fornecer recurso para o transporte de múltiplas VLAN por uma única porta (ou por um conjunto agregado de portas) utilizando o protocolo 802.1q;

1.1.20.232. Possuir suporte a IPv6;

1.1.20.233. A solução deve suportar múltiplas tabelas de rotas independentes;

1.1.20.234. A solução deve possuir suporte a múltiplos domínios de roteamento em IPv4 e IPv6;
1.1.20.236. Possuir ferramenta online web gratuita na qual seja possível carregar as configurações e

receber diagnóstico da solução com informações sobre atualizações, melhores práticas, estado

da solução e informações preventivas.

1.1.20.237. A solução deve operar em, no mínimo, a seguintes formas:

1.1.20.238. DNS autoritativo;

1.1.20.239. DNS secundário;

1.1.20.240. DNS resolver;

1.1.20.241. DNS cache;

1.1.20.242. Balanceamento de DNS servers;

1.1.20.243. DNSSec;

1.1.20.244. A solução deve ser capaz de realizar transferência de zonas para múltiplos servidores DNS Primários responsáveis por diferentes zonas.

1.1.20.245. Deve possuir funcionalidade de DNS cache, realizando cache transparente, caching resolver e validação de caching resolver.

1.1.20.246. Capacidade de uso de chave criptográfica TSIG para comunicação segura entre servidores DNS, obedecendo no mínimo os padrões: HMAC MD5, HMAC SHA-1 ou HMAC SHA-256;

1.1.20.247. A solução deve realizar o offload dos servidores de DNS, funcionando como o DNS secundário;

1.1.20.248. A solução deve servir as respostas as requisições onde o DNS é o autoritativo a partir da memória RAM;

1.1.20.249. A solução deve possuir proteções contra ataques DNS, no mínimo:

1.1.20.250. Inspeção de protocolo;

1.1.20.251. Validação de protocolo;

1.1.20.252. UDP flood;

1.1.20.253. Pacotes malformados;

1.1.20.254. Ataque teardrop;

1.1.20.255. Ataque ICMP;

1.1.20.256. Permitir que regras customizadas em linguagem aberta possam ser utilizadas para customizar a distribuição dinâmica de tráfego e aumentar a proteção contra ataques;

1.1.20.257. A solução deve ser capaz de realizar balanceamento dos servidores DNS;

1.1.20.258. A solução deve ser capaz de realizar filtragem de pacotes;

1.1.20.259. A solução deve prover segurança do protocolo DNS, protegendo contra ataques de negação de serviço, NXDOMAIN e reflexão de DNS.

1.1.20.260. A solução deve prover segurança do protocolo DNS, protegendo contra ataques de Cache Poisoning.

1.1.20.261. A solução deve realizar stateful inspection;

1.1.20.262. A solução deve possuir base de Geolocalização IP;

1.1.20.263. A solução deve implementar DNS64;

1.1.20.264. A solução deve suportar pelo menos os seguintes tipos de requisição DNS: SOA, A, AAAA, CNAME, DNAME, HINFO, MX, NS, PTR, SRV, TXT

1.1.20.265. Deve ser capaz de gerar estatísticas sobre consultas de DNS por: Aplicação, nome da query, tipo da query, endereço IP do cliente;

1.1.20.266. Deve ser possível configurar a solução de modo inline a estrutura de DNS existente e transparente sem requerer grandes mudanças na infraestrutura;

1.1.20.267. Deve prover as respostas a queries DNS da própria RAM CACHE

1.1.20.268. A solução deve ser capaz de realizar IP Anycast;

1.1.20.269. A solução deve ser capaz de realizar DNSSec, independente da estrutura dos servidores DNS em uso;

1.1.20.270. A solução de alta disponibilidade não deve depender de BGP ou outro protocolo de roteamento;

1.1.20.271. A solução de alta disponibilidade será realizada baseada em respostas a requisições DNS. A resposta a requisições DNS devem conter apenas endereços que estejam disponíveis no momento, e balanceadas por usuário, de acordo com as políticas definidas;

1.1.20.272. A solução deverá aceitar resolução de nomes baseada em topologia, onde requisições de DNS são respondidas baseado no país, continente, ou endereço IP de onde veio a requisição;

1.1.20.273. Deve ser possível ajustar quantos endereços são enviados em uma única resposta;
1.1.20.274. Suporte a monitoração de estado de saúde de servidores, serviços e links de conexão a provedor de serviço, garantindo a disponibilidade do serviço oferecido entre datacenters;

1.1.20.275. Deve possuir suporte a monitoração de pelo menos 15 diferentes aplicações, incluindo SAP, Oracle, mySQL e LDAP.

1.1.20.276. Suportar pelo menos os seguintes algoritmos de balanceamento global:

1.1.20.277. Round Robin;

1.1.20.278. Global Availability;

1.1.20.279. Ratio;

1.1.20.280. LDNS Persist;

1.1.20.281. Geografia;

1.1.20.282. Disponibilidade da Aplicação;

1.1.20.283. Capacidade do Virtual Server;

1.1.20.284. Least Connections;

1.1.20.285. Pacotes por segundo;

1.1.20.286. Round trip time;

1.1.20.287. Hops;

1.1.20.288. Packet Completion Rate;

1.1.20.289. QoS definido pelo usuário;

1.1.20.290. Kilobytes per Second;

1.1.20.291. Implementar persistência da conexão do usuário entre aplicações ou data centers;
1.1.20.292. A solução deverá suportar o controle de grupos de aplicações, e permitir que um usuário seja redirecionado para outro datacenter quando houver falha em qualquer das aplicações de um mesmo grupo;

1.1.20.293. A solução deverá permitir que as políticas sejam configuradas individualmente por aplicação sendo balanceada;

1.1.20.294. A solução deverá permitir que a contingência seja automática, mas que o retorno seja manual;

1.1.20.295. A solução deve ser capaz de lidar com clientes IPv6 quando o site atende apenas com IPv4 (requests AAAA ou A6);

1.1.20.296. Possuir suporte a IPv6 no balanceamento global entre datacenters.

1.1.20.297. Ter capacidade de tratar informações das camadas L4-L7 (FTP, SMTP, URL, HTTP Header, TCP e UDP) para a tomada de decisão de encaminhamento a servidor real, em IPv4 e IPv6.

1.1.20.298. Deverá possuir a funcionalidade de resposta rápida a queries DNS. permitindo respostas mais rápidas para zonas que seja autoritativo.

1.1.20.299. A solução deve possuir suporte a Response Policy Zones (RPZ), mecanismo de firewall usado por DNS recursivo para permitir o tratamento customizado da resolução de nomes. Portanto a solução deve ser capaz de filtrar queries DNS para domínios considerados maliciosos e retornar respostas customizadas.

1.1.20.300. A solução deve possuir linguagem de programação open-source que permita a manipulação do tráfego de entrada e saída, viabilizando assim a alteração de parâmetros no cabeçalho e no corpo das mensagens.

1.1.20.301. Essa linguagem de programação deve permitir a importação de pacotes, garantindo assim que a agilidade e flexibilidade no compartilhamento dos scripts.

1.1.20.302. Deve estender a funcionalidade de programabilidade com Node.js, provendo um ambiente para rodar JavaScript independente de web browser.

1.1.21. ITEM 21 – FIREWALL DE APLICAÇÃO WEB – WAF – DATACENTER TIPO II

1.1.21.1. Os appliances físicos devem ser novos e de primeiro uso;

1.1.21.2. Os equipamentos devem ser fornecidos em modo appliance, com conjunto de hardware e software dedicados, não podendo ser servidor de uso genérico, e que atendam todas as funcionalidades descritas neste Termo de Referência;

1.1.21.3. Devem ser novos, sem uso prévio e entregues em perfeito estado de funcionamento. Não devem ser remanufaturados, recondicionados ou possuir reparos de qualquer espécie;

1.1.21.4. Não serão aceitos equipamentos ou softwares que constem em anúncio ou lista do tipo end-of-sale, end-of-support ou end-of-life do fabricante, ou seja, produtos que serão descontinuados, perderão suporte e garantia oficiais do fabricante;

1.1.21.5. Deverão ser fornecidos todos os cabos, suportes (se necessários, "gavetas", "braços" e "trilhos"), incluindo todos os cabos de ligação lógica e elétrica necessários à instalação e perfeito funcionamento do equipamento no rack;

1.1.21.6. Dispor de fonte de alimentação redundante com tensão de entrada de 110V a 220V AC automática e frequência de 60Hz;

1.1.21.7. Possuir sistema operacional customizado especificamente para funções de Web Application Firewall, não podendo ser entregue appliance do tipo NGFW;

1.1.21.8. A solução deve ser licenciada para uso perpétuo. As funcionalidades da solução devem permanecer ativas após o período de garantia mesmo que desatualizadas e com todas as atualizações e assinaturas que forem disponibilizadas até data final do período que foram aplicadas ou instaladas na solução;

1.1.21.9. Possuir, no mínimo, 08 (oito) interfaces de 10GE SFP+. Serão aceitas interfaces de maior capacidade, desde que possibilitem ser transformados em 10 GE (incluindo os cabos “breakout” de no mínimo 3 metros);

1.1.21.10. Possuir, pelo menos, 02 (duas) interfaces 100G/40G QSFP+/QSFP28;

1.1.21.11. Possuir 01 interfaces 1GE, incluso interfaces de gerência com conectores padrão RJ45;

1.1.21.12. Todas as interfaces fornecidas devem estar licenciadas e habilitadas para uso imediato;

1.1.21.13. Deve possuir capacidade de inspecionar, no mínimo, 82 (oitenta e dois) Gbps de tráfego web em camada 7;

1.1.21.14. Suportar no mínimo 45.000 (quarenta e cinco mil) transações por segundo (TPS) SSL utilizando curva elíptica (ECDHE) com chaves RSA 2048 bits;

1.1.21.15. Suportar 80.000.000 (oitenta milhões) de conexões concorrentes em camada 4;

1.1.21.16. Possuir no mínimo compressão de 35.000 Mbps em tráfego HTTP/HTTPS;

1.1.21.17. Recursos de agregação de portas baseado no protocolo LACP, segundo o padrão IEEE 802.3ad;

1.1.21.18. Memória RAM mínima de 128 GB;

1.1.21.19. Disco rígido com capacidade de armazenamento interno e retenção de logs para análise com capacidade mínima de 1TB;

1.1.21.20. Deve vir acompanhado de todas as licenças de software ou hardware necessárias para atendimento das funcionalidades exigidas neste caderno de especificações técnicas;

1.1.21.21. Garantir que na aceleração de SSL, tanto a troca de chaves quanto a criptografia dos dados seja realizada com aceleração em hardware, para não onerar o sistema;

1.1.21.22. Deve permitir a configuração da solução em alta disponibilidade, permitindo o funcionamento em cluster do tipo ativo-passivo e ativo-ativo;

1.1.21.23. A solução deve suportar mais do que dois elementos no cluster para sincronização de

configuração de forma nativa a fim de permitir escalabilidade no futuro;

1.1.21.24. Implementar a sincronização entre os equipamentos redundantes, assegurando que não haverá "downtime" e queda de sessões em caso de falha de uma das unidades;

1.1.21.25. Possuir recurso para o transporte de múltiplas VLANs por uma única porta (ou por um conjunto agregado de portas) utilizando o protocolo 802.1q;

1.1.21.26. Deve suportar, no mínimo, 1000 VLANs simultaneamente;

1.1.21.27. Analisar e proteger tráfego HTTP/1.0, HTTP/1.1, HTTP/2.0 e/ou HTTP/3;

1.1.21.28. Possuir suporte a IPv6;

1.1.21.29. A solução deve permitir o encapsulamento, em camada 3, do tráfego entre o balanceador e o servidor para tráfego IPv4 e IPv6, quando o balanceamento é realizado apenas em direção ao servidor, onde a resposta do servidor real é enviada diretamente ao cliente;

1.1.21.30. Possuir suporte à funcionalidade de VXLAN para integração com o ambiente de virtualização (Software Defined Network);

1.1.21.31. Assinar cookies digitalmente e editar endereços de URL (“URL Rewriting”);

1.1.21.32. Os usuários de gerência deverão poder ser autenticados em bases remotas. No mínimo RADIUS, LDAP e TACACS+ deverão ser suportados;

1.1.21.33. Deverá possuir uma funcionalidade de criação automática de políticas, para proteção DDOS e ataques zero-day onde a política de segurança é criada e atualizada automaticamente baseando-se no tráfego real observado à aplicação;

1.1.21.34. Restringir métodos HTTP/ HTTPS permitidos, tipos ou versões de protocolos, tipos de caracteres e versões utilizadas de cookies;

1.1.21.35. Permitir as seguintes opções de implementação:

1.1.21.36. Monitoramento (sem bloqueio);

1.1.21.37. Proxy (reverso e transparente);

1.1.21.38. Permitir que novas políticas fiquem apenas monitorando o tráfego, sem bloqueá-lo, indicando caso aconteça algum evento;

1.1.21.39. Remover as mensagens de erro do conteúdo que será enviado aos usuários;

1.1.21.40. Proteger contra-ataques automatizados, incluindo bots e web scraping, identificando comportamento não humano, navegadores operados por scripts ou qualquer outra forma que não operados por humanos;

1.1.21.41. Possuir firewall XML integrado com suporte a filtro e validação de funções XML específicas da aplicação;

1.1.21.42. A solução deve suportar e fazer a proteção do tráfego de protocolo WebSocket;

1.1.21.43. Permitir a utilização de modelo positivo de segurança para proteger contra ataques às aplicações HTTP e HTTPS, além de proteção contra- ataques conhecidos aos protocolos HTTP e HTTPS;

1.1.21.44. Criação de políticas automáticas que bloqueiam o endereço IP que realizar violações;

1.1.21.45. Possuir mecanismo de aprendizado automatizado capaz de identificar todos os conteúdos das aplicações, incluindo URLs, parâmetros URLs, campos de formulários, o que se espera de cada campo (tipo de dado, tamanho de caracteres, se é um campo obrigatório), cookies, ações SOAP e elementos XML. Identificar e criar perfil de utilização dos aplicativos, inclusive desenvolvidos em Javascript, CGI, ASP e PHP;

1.1.21.46. Deve possuir tecnologia para mitigação de DDoS em camada 7 baseado em análise

comportamental, usando o aprendizado;

1.1.21.47. A solução deve possuir a capacidade de capturar tráfego no formato TCP Dump relativos a ataques DoS L7, Web Scraping e força bruta permitindo uma análise mais aprofundada por parte do administrador;

1.1.21.48. Detectar ataques de força bruta por meio dos seguintes métodos:

1.1.21.49. Aumento do tempo de resposta da aplicação monitorada ou bloqueio temporário do atacante;

1.1.21.50. Quantidade de transações por segundo (TPS), monitorando a quantidade de transações por segundo por endereço IP;

1.1.21.51. Permitir a criação de políticas diferenciadas por aplicação e por URL, onde cada aplicação e URL poderão ter políticas totalmente diferentes;

1.1.21.52. Apresentar proteção contra-ataques, como:

1.1.21.53. Brute Force Login;

1.1.21.54. Buffer Overflow;

1.1.21.55. Cookie Injection;

1.1.21.56. Cookie Poisoning;

1.1.21.57. Cross Site Request Forgery (CSRF);

1.1.21.58. Cross Site Scripting (XSS);

1.1.21.59. Server Side Request Forgery (SSRF);

1.1.21.60. Directory Traversal;

1.1.21.61. Forceful Browsing;

1.1.21.62. HTTP Denial of Service;

1.1.21.63. HTTP hidden field manipulation;

1.1.21.64. HTTP request smuggling;

1.1.21.65. HTTP Response Splitting;

1.1.21.66. Malicious Robots;

1.1.21.67. Parameter Tampering;

1.1.21.68. Remote File Inclusion Attacks;

1.1.21.69. Sensitive Data Leakage (Social Security Numbers, Cardholder Data, PII, HPI);

1.1.21.70. Session Hijacking;

1.1.21.71. SQL Injection;

1.1.21.72. Web Scraping;

1.1.21.73. Web server software and operating system attacks;

1.1.21.74. Web Services (XML) attacks;

1.1.21.75. Deve permitir que possa ser especificado na política os tipos de arquivos que serão bloqueados (File Types);

1.1.21.76. A solução deve permitir a inspeção de upload de arquivos para os servidores de aplicação, ou enviar para inspeção através do protocolo ICAP;

1.1.21.77. Deve encriptar dados e credenciais na camada de aplicação, sem ter a necessidade de atualizar a aplicação. Essas informações devem ser encriptadas para proteger o login e as

credenciais dos usuários e com isso os dados da aplicação;

1.1.21.78. Deve proteger informações sensíveis e confidenciais da interceptação por terceiros, através da criptografia de dados quando ainda no browser do usuário. Deve proteger esses dados criptografados de malwares e keyloggers;

1.1.21.79. Deve ofuscar o nome de um parâmetro sensível da aplicação em caracteres randômicos. Esse nome de parâmetro deve ser mudado constantemente pela ferramenta para dificultar ataques direcionados;

1.1.21.80. A solução deve fornecer relatórios consolidados de ataques com pelo menos os seguintes dados:

1.1.21.81. Resumo geral com as políticas ativas, anomalias e estatísticas de tráfego, Ataques DoS, Ataques de Força Bruta, Ataques de Robôs, Violações, URL, Endereços IP, Países, Severidade;

1.1.21.82. Deverá permitir o agendamento de relatórios a serem entregues por email;

1.1.21.83. Emitir os seguintes relatórios gráficos por:

1.1.21.84. Política de segurança;

1.1.21.85. Tipos de ataques;

1.1.21.86. Violações;

1.1.21.87. URL que foram atacadas;

1.1.21.88. Endereços IP de origem;

1.1.21.89. Localização geográfica dos endereços IPs de origem;

1.1.21.90. Severidade;

1.1.21.91. Código de resposta;

1.1.21.92. Métodos;

1.1.21.93. Protocolos;

1.1.21.94. Sessão;

1.1.21.95. A solução deve ser capaz de proteger GraphQL APIs com pelos menos os seguintes parâmetros: tamanho total, tamanho de cada parâmetro

1.1.21.96. A solução deve ser capaz de proteger GraphQL APIs limitando a quantidade de queries dentro de uma requisição HTTP

1.1.21.97. A solução deve ser capaz de proteger APIs baseadas em OpenAPI 2.0

1.1.21.98. A solução deve ser capaz de proteger APIs baseadas em OpenAPI 3.0

1.1.21.99. A solução deve suportar a criação de políticas de proteção com base no modelo OWASP, onde pelo menos devem ser aplicadas políticas de proteção contra o TOP 10 OWASP

1.1.21.100. A solução deve emitir relatório com análise cada política de proteção comparado com o TOP 10 OWASP.

1.1.21.101. A solução deverá possuir as seguintes formas de detecção de ataques DoS na camada de aplicação:

1.1.21.102. Número de requisições por segundo enviados a uma URL específica;

1.1.21.103. Número de requisições por segundo enviados de um IP específico;

1.1.21.104. Detecção através de código executado no cliente com o objetivo de detectar interação humana ou comportamento de robôs (bots);

1.1.21.105. Número máximo de transações por segundo (TPS) de um determinado IP;

1.1.21.106. Aumento de um determinado percentual do número de transações por segundo (TPS);
1.1.21.107. Aumento do stress do servidor de aplicação;

1.1.21.108. Funcionalidades de Balanceamento de Carga

1.1.21.109. Deve suportar todas as aplicações comuns de um Switch Layer 7, como:

1.1.21.110. Server Load-Balancing;

1.1.21.111. Firewall Load-Balancing;

1.1.21.112. Proxy Load-Balancing;

1.1.21.113. Deve suportar balanceamento apenas em direção ao servidor, onde a resposta do servidor real é enviada diretamente ao cliente;

1.1.21.114. Deve permitir o encapsulamento, em camada 3, do tráfego entre a solução e o servidor para tráfego IPv4 e IPv6, quando o balanceamento é realizado apenas em direção ao servidor, onde a resposta do servidor real é enviada diretamente ao cliente;

1.1.21.115. Permitir a clonagem de pools, de forma que a solução envie uma cópia do tráfego para um pool adicional, como por exemplo um pool de IDSs ou Sniffers, para fins de análise de tráfego de rede ou mesmo para identificação de padrões de acesso não permitidos ou indicações de atividade maliciosas ou ataques de rede;

1.1.21.116. Possuir recursos para balancear servidores com qualquer hardware, sistema operacional e tipo de aplicação;

1.1.21.117. A solução deve possuir recurso de ativação de grupo prioritário, no qual o administrador pode especificar a quantidade mínima de servidores que devem estar disponíveis em cada grupo e a prioridade dos grupos.

1.1.21.118. Caso o número de servidores disponíveis fique menor do que o estipulado pelo administrador, a solução deve automaticamente distribuir o tráfego para o próximo grupo com maior prioridade não afetando o serviço.

1.1.21.119. Caso o número de servidores disponíveis volte ao valor mínimo estipulado pelo administrador, a solução deve automaticamente retirar o grupo com menor prioridade de balanceamento, voltando ao estado original.

1.1.21.120. Possuir capacidade de abrir um número reduzido de conexões TCP com o servidor e inserir os HTTP requests gerado pelos clientes nestas conexões, reduzindo a necessidade de estabelecimento de conexões nos servidores e aumentando a performance do serviço;

1.1.21.121. Suportar os seguintes métodos de balanceamento:

1.1.21.122. Round Robin;

1.1.21.123. Least Connections;

1.1.21.124. Weighted Percentage (por peso);

1.1.21.125. Servidor ou equipamento com resposta mais rápida baseado no tráfego real;

1.1.21.126. Weighted Percentage dinâmico (baseado no número de conexões)

1.1.21.127. Dinâmico, baseado em parâmetros de um determinado servidor ou equipamento, coletados via SNMP ou WMI;

1.1.21.128. A solução deve permitir aplicar criptografia de cookies para a poteção dos cookies utilizados pela aplicação web;

1.1.21.129. Possuir recursos para balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência de sessão dos seguintes tipos:

1.1.21.130. Por cookie: inserção de um novo cookie na sessão;

1.1.21.131. Por cookie: utilização do valor do cookie da aplicação, sem adição de cookie;
1.1.21.132. Por endereço IP destino;

1.1.21.133. Por endereço IP origem;

1.1.21.134. Por sessão SSL;

1.1.21.135. Através da análise da URL acessada.;

1.1.21.136. Através da análise de qualquer parâmetro no header HTTP;

1.1.21.137. Através da análise do MS Terminal Services Session (MSRDP)

1.1.21.138. Através da análise do SIP Call ID ou Source IP;

1.1.21.139. Através da análise de qualquer informação da porção de dados (camada 7);

1.1.21.140. A solução deve utilizar Cache Array Routing Protocol (CARP) no algoritmo de HASH;
1.1.21.141. Deve suportar os seguintes métodos de monitoramento dos servidores reais:

1.1.21.142. ICMP;

1.1.21.143. Conexões TCP e UDP pela respectiva porta no servidor;

1.1.21.144. Devem existir monitores predefinidos para, no mínimo, os seguintes protocolos: ICMP, HTTP, HTTPS, Diameter, FTP, SASP, SMB, RADIUS, MSSQL, NNTP, ORACLE, RPC, LDAP, IMAP, SMTP, POP3, SIP, Real Server, SOAP, SNMP e WMI;

1.1.21.145. Possuir recursos para balanceamento de carga de servidores SIP para VoIP (equipamento SIP PROXY);

1.1.21.146. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor físico

1.1.21.147. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor virtual;

1.1.21.148. Possuir recursos para limitar o número de sessões estabelecidas com cada grupo de servidores;

1.1.21.149. Realizar Network Address Translation (NAT);

1.1.21.150. Realizar Proteção contra Denial of Service (DoS);

1.1.21.151. Realizar Proteção contra Syn flood;

1.1.21.152. Realizar Limpeza de cabeçalho HTTP;

1.1.21.153. Deve permitir o controle da resposta ICMP por servidor virtual;

1.1.21.154. Possuir recursos para que a configuração seja baseada em perfis, permitindo uma fácil administração;

1.1.21.155. Possuir capacidade de geração e gestão de perfis hierarquizados, permitindo maior facilidade na administração de políticas similares;

1.1.21.156. Permitir a criação de Virtual Servers com endereço IPv4 e os servidores reais com endereços IPv6;

1.1.21.157. Possuir recursos para executar compressão de conteúdo HTTP, para reduzir a quantidade de informações enviadas ao cliente;

1.1.21.158. Definir qual tipo de compressão será habilitada (gzip1 a gzip9, deflate);

1.1.21.159. Possuir capacidade para definir compressão especificamente para certos tipos de objetos;

1.1.21.160. Permitir a utilização de memória RAM como cache de objetos HTTP, para responder às

requisições dos usuários sem utilizar recursos dos servidores;

1.1.21.161. Permitir definir quais tipos de objeto serão armazenados em cache e quais nunca devem ser cacheados;

1.1.21.162. Garantir que o recurso de cache possa ajustar quanta memória será utilizada para armazenar objetos;

1.1.21.163. Suporte a otimização do protocolo TCP para ajustes a parâmetros das conexões clientes e servidor;

1.1.21.164. Deve possuir relatórios das aplicações, com pelos menos os seguintes gráficos: 1.1.21.165. Tempo de resposta da aplicação;

1.1.21.166. Latência ;

1.1.21.167. Conexões para conjunto de servidores, servidores individuais;

1.1.21.168. Por URL;

1.1.21.169. A ferramenta de relatórios deve possuir pelo menos os seguintes filtros para a geração dos gráficos:

1.1.21.170. Servidores virtuais

1.1.21.171. Servidores balanceados

1.1.21.172. URLs

1.1.21.173. Países de origem, baseados em geolocalização (GEOIP)

1.1.21.174. Dispositivos de origem do cliente (user agent)

1.1.21.175. Deve possuir framework unificado para configuração da aplicação

1.1.21.176. Quando licenciada, a solução deve ter a capacidade de realizar cache transparente das respostas DNS;

1.1.21.177. A Solução deve ter suporte a sFlow;

1.1.21.178. A solução deve possuir múltiplos domínios de roteamento em IPv4 e IPv6;

1.1.21.179. A solução deve permitir que cada domínio de roteamento utilize BGP, OSPF e RIP em IPv4 e IPv6;

1.1.21.180. A solução deve suportar Equal Cost Multipath (ECMP);

1.1.21.181. A solução deve realizar Bidirectional Forward Detection (BFD);

1.1.21.182. A solução deve ter suporte a Stream Control Transmission Protocol (SCTP);

1.1.21.183. Deve ter suporte a Transport Layer Security (TLS) Server Name Indication (SNI);

1.1.21.184. A solução deve possuir monitor HTTP/HTTPS com autenticação NTLM embutida, que permita verificar se o HTTP/HTTPS está operando assim como a plataforma de autenticação;

1.1.21.185. A solução deve ter suporte a TLS 1.2, SHA 2 Cipher e SHA256 hash;

1.1.21.186. A solução deve ter suporte a criptografia Perfect Forward Secrecy não apenas para troca de chaves RSA.

1.1.21.187. A solução deve ser capaz de colocar em fila as requisições TCP que excedam a capacidade de conexões do grupo de servidores ou de um servidor. A solução não deverá descartar as conexões que excedam o número de conexões do servidor ou do grupo de servidores:

1.1.21.188. Deve ser possível configurar o tamanho máximo da fila;

1.1.21.189. Deve ser possível configurar o tempo máximo de permanência na fila;

1.1.21.190. A solução deve realizar Controle de Banda Estático para grupos de aplicações e rede;
1.1.21.191. A solução deve realizar Controle de Banda Dinâmico por aplicação e usuário;
1.1.21.192. A solução deve realizar Controle de Banda baseado em domínio de roteamento;

1.1.21.193. Permitir tráfego por parâmetros de QoS (Quality of Service) ou rate-shaping, com pelo menos 2 (duas) filas para priorização de tráfego baseada na camada de aplicação;

1.1.21.194. Através dessa priorização de tráfego e restrição de largura de banda deverá ser possível permitir um melhor nível de serviço para clientes preferenciais em detrimento dos demais clientes.

1.1.21.195. A solução deve permitir a priorização de tráfego de entrada para determinadas aplicações.

1.1.21.196. A solução deve permitir a criação de túneis IP por domíno de roteamento utilizando GRE, IPIP, EtherIP, PPP;

1.1.21.197. A solução deve permitir a criação de túneis IP transparente utilizando GRE e IPIP;
1.1.21.198. Fornecer recursos para o uso de servidores (reals) no mesmo Virtual Server;

1.1.21.199. Possuir suporte ao protocolo SPDY e HTTP 2.0;

1.1.21.200. O equipamento deve possuir suporte ao espelhamento de conexões FTP, Telnet, HTTP, UDP, SSL.

1.1.21.201. O equipamento deverá permitir a sincronização das configurações:

1.1.21.202. De forma automática; e

1.1.21.203. Manualmente, forçando a sincronização apenas no momento desejado;

1.1.21.204. Permitir que regras customizadas em linguagem aberta possam ser utilizadas para customizar a distribuição dinâmica de tráfego e aumentar a proteção contra ataques;

1.1.21.205. A solução deve possuir linguagem de programação open-source que permita a manipulação do tráfego de entrada e saída, viabilizando assim a alteração de parâmetros no cabeçalho e no corpo das mensagens.

1.1.21.206. Essa linguagem de programação deve permitir a importação de pacotes, garantindo assim que a agilidade e flexibilidade no compartilhamento dos scripts.

1.1.21.207. Permitir a criação de políticas através de interface gráfica web para manipulação de tráfego através de lógica para pelo menos os seguintes operadores:

1.1.21.208. GEOIP, http-basic-auth, http-cookie, http-header, http-host, http-method, http-referer, http- set-cookie, http-status, http-uri e http-version

1.1.21.209. Deve ser possível tomar as seguintes ações através dessas políticas:

1.1.21.210. Bloqueio de tráfego

1.1.21.211. Reescrita e manipulação de URL

1.1.21.212. Registro de tráfego (log)

1.1.21.213. Adição de informação no cabeçalho HTTP

1.1.21.214. Redirecionamento do tráfego para um membro específico

1.1.21.215. Selecionar uma política específica para Aplicação Web

1.1.21.216. A solução deverá ser capaz de fazer log de todas as sessões, onde os registros deverão conter:

1.1.21.217. Endereço IP de origem;

1.1.21.218. Porta TCP ou UDP de origem;

1.1.21.219. Endereço IP de destino;

1.1.21.220. Porta TCP ou UDP de destino;

1.1.21.221. Protocolo de camada 4 (TCP ou UDP);

1.1.21.222. Data e hora da mensagem;

1.1.21.223. URL acessada;

1.1.21.224. A solução deve possuir políticas de uso de senhas administrativas tais como: nível de complexidade, período de validade e travamento de conta devido a erros múltiplos de login de forma nativa ou no mínimo integrado a uma base Active Directory.

1.1.21.225. A solução deve suportar controle de versão da política de configuração de forma a permitir fazer roll back de políticas aplicadas.

1.1.21.226. Funcionalidades para alta disponibilidade entre ambientes de Datacenter

1.1.21.227. Fornecer recurso de agregação de portas baseado no protocolo LACP;

1.1.21.228. Deve possuir suporte a LACP em modo passivo e ativo;

1.1.21.229. Fornecer recurso para suportar até 8 portas em um mesmo conjunto agregado;

1.1.21.230. Deve possuir suporte a Spanning-Tree(802.1D), Fast Spanning-Tree (802.1w, 802.1t) e Multi Spanning-Tree (802.1s);

1.1.21.231. Fornecer recurso para o transporte de múltiplas VLAN por uma única porta (ou por um conjunto agregado de portas) utilizando o protocolo 802.1q;

1.1.21.232. Possuir suporte a IPv6;

1.1.21.233. A solução deve suportar múltiplas tabelas de rotas independentes;

1.1.21.234. A solução deve possuir suporte a múltiplos domínios de roteamento em IPv4 e IPv6;
1.1.21.235. Possuir ferramenta online web gratuita na qual seja possível carregar as configurações e receber diagnóstico da solução com informações sobre atualizações, melhores práticas, estado da solução e informações preventivas.

1.1.21.236. A solução deve operar em, no mínimo, a seguintes formas:

1.1.21.237. DNS autoritativo;

1.1.21.238. DNS secundário;

1.1.21.239. DNS resolver;

1.1.21.240. DNS cache;

1.1.21.241. Balanceamento de DNS servers;

1.1.21.242. DNSSec;

1.1.21.243. A solução deve ser capaz de realizar transferência de zonas para múltiplos servidores DNS Primários responsáveis por diferentes zonas.

1.1.21.244. Deve possuir funcionalidade de DNS cache, realizando cache transparente, caching resolver e validação de caching resolver.

1.1.21.245. Capacidade de uso de chave criptográfica TSIG para comunicação segura entre servidores DNS, obedecendo no mínimo os padrões: HMAC MD5, HMAC SHA-1 ou HMAC SHA-256;

1.1.21.246. A solução deve realizar o offload dos servidores de DNS, funcionando como o DNS

secundário;

1.1.21.247. A solução deve servir as respostas as requisições onde o DNS é o autoritativo a partir da memória RAM;

1.1.21.248. A solução deve possuir proteções contra ataques DNS, no mínimo:

1.1.21.249. Inspeção de protocolo;

1.1.21.250. Validação de protocolo;

1.1.21.251. UDP flood;

1.1.21.252. Pacotes malformados;

1.1.21.253. Ataque teardrop;

1.1.21.254. Ataque ICMP;

1.1.21.255. Permitir que regras customizadas em linguagem aberta possam ser utilizadas para customizar a distribuição dinâmica de tráfego e aumentar a proteção contra ataques;

1.1.21.256. A solução deve ser capaz de realizar balanceamento dos servidores DNS;

1.1.21.257. A solução deve ser capaz de realizar filtragem de pacotes;

1.1.21.258. A solução deve prover segurança do protocolo DNS, protegendo contra ataques de negação de serviço, NXDOMAIN e reflexão de DNS.

1.1.21.259. A solução deve prover segurança do protocolo DNS, protegendo contra ataques de Cache Poisoning.

1.1.21.260. A solução deve realizar stateful inspection;

1.1.21.261. A solução deve possuir base de Geolocalização IP;

1.1.21.262. A solução deve implementar DNS64;

1.1.21.263. A solução deve suportar pelo menos os seguintes tipos de requisição DNS: SOA, A, AAAA, CNAME, DNAME, HINFO, MX, NS, PTR, SRV, TXT

1.1.21.264. Deve ser capaz de gerar estatísticas sobre consultas de DNS por: Aplicação, nome da query, tipo da query, endereço IP do cliente;

1.1.21.265. Deve ser possível configurar a solução de modo inline a estrutura de DNS existente e transparente sem requerer grandes mudanças na infraestrutura;

1.1.21.266. Deve prover as respostas a queries DNS da própria RAM CACHE;

1.1.21.267. A solução deve ser capaz de realizar IP Anycast;

1.1.21.268. A solução deve ser capaz de realizar DNSSec, independente da estrutura dos servidores DNS em uso;

1.1.21.269. A solução de alta disponibilidade não deve depender de BGP ou outro protocolo de roteamento;

1.1.21.270. A solução de alta disponibilidade será realizada baseada em respostas a requisições DNS. A resposta a requisições DNS devem conter apenas endereços que estejam disponíveis no momento, e balanceadas por usuário, de acordo com as políticas definidas;

1.1.21.271. A solução deverá aceitar resolução de nomes baseada em topologia, onde requisições de DNS são respondidas baseado no país, continente, ou endereço IP de onde veio a requisição;

1.1.21.272. Deve ser possível ajustar quantos endereços são enviados em uma única resposta;
1.1.21.273. Suporte a monitoração de estado de saúde de servidores, serviços e links de conexão a

provedor de serviço, garantindo a disponibilidade do serviço oferecido entre datacenters;

1.1.21.274. Deve possuir suporte a monitoração de pelo menos 15 diferentes aplicações, incluindo SAP, Oracle, mySQL e LDAP.

1.1.21.275. Suportar pelo menos os seguintes algoritmos de balanceamento global: 1.1.21.276. Round Robin;

1.1.21.277. Global Availability;

1.1.21.278. Ratio;

1.1.21.279. LDNS Persist;

1.1.21.280. Geografia;

1.1.21.281. Disponibilidade da Aplicação;

1.1.21.282. Capacidade do Virtual Server;

1.1.21.283. Least Connections;

1.1.21.284. Pacotes por segundo;

1.1.21.285. Round trip time;

1.1.21.286. Hops;

1.1.21.287. Packet Completion Rate;

1.1.21.288. QoS definido pelo usuário;

1.1.21.289. Kilobytes per Second;

1.1.21.290. Implementar persistência da conexão do usuário entre aplicações ou data centers; 1.1.21.291. A solução deverá suportar o controle de grupos de aplicações, e permitir que um usuário seja redirecionado para outro datacenter quando houver falha em qualquer das aplicações de um mesmo grupo;

1.1.21.292. A solução deverá permitir que as políticas sejam configuradas individualmente por aplicação sendo balanceada;

1.1.21.293. A solução deverá permitir que a contingência seja automática, mas que o retorno seja manual;

1.1.21.294. A solução deve ser capaz de lidar com clientes IPv6 quando o site atende apenas com IPv4 (requests AAAA ou A6);

1.1.21.295. Possuir suporte a IPv6 no balanceamento global entre datacenters.

1.1.21.296. Ter capacidade de tratar informações das camadas L4-L7 (FTP, SMTP, URL, HTTP Header, TCP e UDP) para a tomada de decisão de encaminhamento a servidor real, em IPv4 e IPv6.

1.1.21.297. Deverá possuir a funcionalidade de resposta rápida a queries DNS. permitindo respostas mais rápidas para zonas que seja autoritativo.

1.1.21.298. A solução deve possuir suporte a Response Policy Zones (RPZ), mecanismo de firewall usado por DNS recursivo para permitir o tratamento customizado da resolução de nomes. Portanto a solução deve ser capaz de filtrar queries DNS para domínios considerados maliciosos e retornar respostas customizadas.

1.1.21.299. A solução deve possuir linguagem de programação open-source que permita a manipulação do tráfego de entrada e saída, viabilizando assim a alteração de parâmetros no cabeçalho e no corpo das mensagens.

1.1.21.300. Essa linguagem de programação deve permitir a importação de pacotes, garantindo

assim que a agilidade e flexibilidade no compartilhamento dos scripts.

1.1.21.301. Deve estender a funcionalidade de programabilidade com Node.js, provendo um ambiente para rodar JavaScript independente de web browser.

1.1.22. ITEM 22 - INSTALAÇÃO DE FIREWALL UNIDADE ATÉ 100KM

1.1.22.1. Instalação e Configuração de Firewall dos itens 1 a 4 em localidade até 100km distante de Fortaleza

1.1.22.2. A instalação deve ser feita conforme item 2 deste TR.

1.1.23. ITEM 23 - INSTALAÇÃO DE FIREWALL UNIDADE ATÉ 400KM

1.1.23.1. Instalação e Configuração de Firewall dos itens 1 a 4 em localidade de 100 km até 400 km distante de Fortaleza

1.1.23.2. A instalação deve ser feita conforme item 2 deste TR.

1.1.24. ITEM 24 - INSTALAÇÃO DE FIREWALL UNIDADE ACIMA DE 400KM

1.1.24.1. Instalação e Configuração de Firewall dos itens 1 a 4 em localidade mais de 400 km distante de Fortaleza

1.1.24.2. A instalação deve ser feita conforme item 2 deste TR.

1.1.25. ITEM 25 - INSTALAÇÃO FIREWALL SEDE

1.1.25.1. Instalação e Configuração de Firewall dos itens 5 a 7;

1.1.25.2. A instalação deve ser feita conforme item 2 deste TR.

1.1.26. ITEM 26 - INSTALAÇÃO FIREWALL DATA CENTER

1.1.26.1. Instalação e Configuração de Firewall dos itens 8 a 10;

1.1.26.2. A instalação deve ser feita conforme item 2 deste TR.

1.1.27. ITEM 27 – INSTALAÇÃO FIREWALL DE APLICAÇÃO WEB – WAF – VIRTUAL

1.1.27.1. Instalação e Configuração de Firewall de Aplicação Web – Virtual do item 19;

1.1.27.2. A instalação deve ser feita conforme item 2 deste TR.

1.1.28. ITEM 28 – INSTALAÇÃO FIREWALL DE APLICAÇÃO WEB – WAF – DATACENTER

1.1.28.1. Instalação e Configuração de Firewall de Aplicação Web – Datacenter dos itens 20 e 21;

1.1.28.2. A instalação deve ser feita conforme item 2 deste TR.

1.1.29. ITEM 29 - SERVIÇO DE MONITORAMENTO E SUPORTE TÉCNICO 24X7 DE FIREWALL UNIDADE TIPO 1 E 2 - 36 MESES

1.1.29.1. Monitoramento e Suporte Técnico 24X7 de Firewall dos itens 1 e 2

1.1.29.2. O serviço deve ser prestado conforme item 6.3 deste TR.

1.1.30. ITEM 30 - SERVIÇO DE MONITORAMENTO E SUPORTE TÉCNICO 24X7 DE FIREWALL UNIDADE TIPO 3 E 4 - 36 MESES

1.1.30.1. Monitoramento e Suporte Técnico 24X7 de Firewall dos itens 3 e 4

1.1.30.2. O serviço deve ser prestado conforme item 6.3 deste TR.

1.1.31. ITEM 31 - SERVIÇO DE MONITORAMENTO E SUPORTE TÉCNICO 24X7 DE FIREWALL SEDE - 36 MESES

1.1.31.1. Monitoramento e Suporte Técnico 24X7 de Firewall dos itens 5 a 7;

1.1.31.2. O serviço deve ser prestado conforme item 6.3 deste TR.

1.1.32. ITEM 32 - SERVIÇO DE MONITORAMENTO E SUPORTE TÉCNICO 24X7 DE FIREWALL DATA CENTER -36 MESES

1.1.32.1. Monitoramento e Suporte Técnico 24X7 de Firewall dos itens 8 a 10;

1.1.32.2. O serviço deve ser prestado conforme item 6.3 deste TR.

1.1.33. ITEM 33 – SERVIÇO DE MONITORAMENTO E SUPORTE TÉCNICO 24X7 DE FIREWALL DE APLICAÇÃO WEB – VIRTUAL – 36 MESES

1.1.33.1. Monitoramento e Suporte Técnico 24X7 de Firewall de Aplicação Web do item 19;

1.1.33.2. O serviço deve ser prestado conforme item 6.3 deste TR.

1.1.34. ITEM 34 – SERVIÇO DE MONITORAMENTO E SUPORTE TÉCNICO 24X7 DE FIREWALL DE APLICAÇÃO WEB – DATACENTER – 36 MESES

1.1.34.1. Monitoramento e Suporte Técnico 24X7 de Firewall de Aplicação Web dos itens 20 e 21;

1.1.34.2. O serviço deve ser prestado conforme item 6.3 deste TR.

1.1.35. ITEM 35 - SERVIÇO DE SOC SECURITY OPERATIONS CENTER -24X7 COM SIEM PACO TES DE 200 EPS -36 MESES

1.1.35.1. SERVIÇO DE MONITORAÇÃO E NOTIFICAÇÃO DE INCIDENTES DE SEGURANÇA

1.1.35.1.1. Os recursos destinados à plena utilização e atendimento aos serviços requeridos pela CONTRATANTE deverão ser e estar hospedados em infraestrutura de DATACENTER que possua certificação Uptime Tier III ou compatível, a ser disponibilizada exclusivamente pela LICITANTE vencedora e por conseguida CONTRATADA. Todas as exigências mínimas contidas nos itens abaixo são indispensáveis e o não atendimento a qualquer um desses itens é motivo suficiente para a imediata desclassificação da LICITANTE.

1.1.35.1.2. O serviço deve contemplar dois ou mais Centros de Operações de Segurança (SOC), operando em regime 24x7x365 (vinte e quatro horas por dia, sete dias por semana, todos os dias do ano);

1.1.35.1.3. A CONTRATADA deve prover níveis de segurança elevados, utilizando no SOC ferramentas para garantir a segurança dos dados manipulados, contemplando, no mínimo, os seguintes controles de segurança física e lógica:

1.1.35.1.3.1. Solução de proteção de endpoints;

1.1.35.1.3.2. Controle de acesso físico ao SOC, com a utilização de pelo menos 02 (dois) mecanismos de autenticação, sendo, no mínimo, um deles por biometria;

1.1.35.1.3.3. Monitoramento por sistema interno de TV (CFTV), armazenando as imagens dos últimos 30 (trinta) dias;

1.1.35.1.3.4. Todos os funcionários da CONTRATADA envolvidos na operação ou que possuam acesso às informações do CONTRATANTE devem assinar termo de responsabilidade e sigilo;

1.1.35.1.4. A CONTRATADA deve disponibilizar toda a infraestrutura necessária para o monitoramento dos alertas de segurança realizado por seus analistas, em regime 24 X 7 (24 horas por dia, 7 dias da semana);

1.1.35.1.5. A CONTRATADA deve realizar as ações necessárias para identificação de incidentes de segurança por meio dos dados e alertas monitorados na Solução Integrada de SOC, que podem comprometer a segurança dos serviços e ativos do CONTRATANTE. A CONTRATADA deve analisar eventos detectados, classificar e categorizar conforme definição do CONTRATANTE. Identificar, registrar, escalar e notificar os incidentes de segurança ao CONTRATANTE para tratamento;

1.1.35.1.6. A CONTRATADA é responsável pelas atividades de camada 1 do SOC, que para o

modelo definido corresponde minimamente às atividades relacionadas abaixo:

1.1.35.1.6.1. Definição de linha base (baseline) de forma a entender o comportamento normal do ambiente monitorado, ajustando métricas e limiares de detecção, com o objetivo de reduzir o número de falsos positivos e aumentar a precisão da detecção

1.1.35.1.6.2. Monitoração de alertas de segurança, onde o analista deve decidir se uma análise é necessária. A detecção consiste em avaliar os alertas de segurança dos sensores buscando indicadores de comportamentos maliciosos que ultrapassem os limiares estabelecidos no baseline. A lógica de detecção deve ser ajustada e de senvolvida, podendo passar a utilizar múltiplos eventos e diferentes fontes de dados. Os alertas devem indicar minimamente:

1.1.35.1.6.2.1. Ataques de força bruta com e sem sucesso;

1.1.35.1.6.2.2. Falhas de autenticação que indiquem suspeita de roubo de identidade; 1.1.35.1.6.2.3. Infecção de equipamentos por vírus;

1.1.35.1.6.2.4. Comprometimento de ativos da rede;

1.1.35.1.6.2.5. Realização de ações suspeitas por parte de usuários privilegiados; 1.1.35.1.6.2.6. Alertas de operação de serviços, como interrupções e falhas;

1.1.35.1.6.2.7. Ataques de negação de serviço;

1.1.35.1.6.2.8. Ataques comuns em aplicações WEB, como XSS e SQL injection; Atividades de botnets;

1.1.35.1.6.2.9. Exploração de vulnerabilidades;

1.1.35.1.7. Detecção por análise de logs, onde o analista realiza pesquisas, revisões e análises estatísticas no histórico de log armazenado na Solução Integrada de SOC, com o objetivo de identificar comportamentos e evidências que indiquem atividades maliciosas ou novas ameaças.

1.1.35.1.8. Análise de eventos, onde o analista deve pesquisar informações adicionais que podem estar relacionadas ao evento em análise, que forneçam algum valor investigativo para identificar comportamentos anômalos ou maliciosos. A análise realizada nessa etapa é preliminar, tendo o objetivo de confirmar a ocorrência de um evento de segurança, eliminando falsos positivos confirmados. O resultado da análise pode ser uma das se guintes categorias:

1.1.35.1.8.1. Evento confirmado: os sensores detectaram corretamente uma ameaça válida. Os incidentes confirmados devem ser escalados para a etapa de mitigação da gestão de incidentes;

1.1.35.1.8.2. Falso positivo: ocorre quando o sistema detecta incorretamente uma ameaça ou não existe risco no evento detectado, sendo eventos alertados como maliciosos, mas não são;

1.1.35.1.8.3. Eventos autorizados: são ameaças detectadas corretamente, mas que são aprovadas pela política de segurança, como por exemplo, a análise de vulnerabilidades;

1.1.35.1.8.4. Indeterminado: quando não existe evidência suficiente para confirmar o evento de segurança;

1.1.35.1.9. Registro de análise, todo evento detectado que for selecionado para análise, deve ser registrado no Sistema de Ticket ofertado, incluindo as atividades de investigação. O resultado da análise pode ser a definição de um falso positivo, encerrando o tíquete, ou a confirmação de um incidente de segurança, escalando o tíquete para tratamento. O tíquete deve conter as seguintes informações:

1.1.35.1.9.1. Identificador do ticket;

1.1.35.1.9.2. Sensor que detectou o evento;

1.1.35.1.9.3. Identificador do evento gerado no sensor;

1.1.35.1.9.4. Limiar de detecção utilizado para enviar o evento para análise;

1.1.35.1.9.5. Log do evento detectado;

1.1.35.1.9.6. Origem e categoria do ataque;

1.1.35.1.9.7. Data e hora;

1.1.35.1.10. Triagem e Categorização de eventos, os tíquetes registrados devem ser priorizados por categorias, unificando os eventos potenciais de incidentes com as características em comum, que podem receber tratamento padronizado. Os eventos confirmados, classificados como incidente, devem ter seu tíquete escalado para os analistas do CONTRATANTE;

1.1.35.1.11. Elaboração de relatórios. A CONTRATADA deverá disponibilizar relatórios em formato pdf, referentes aos indicadores monitorados com periodicidade mínima mensal, ou sob demanda, podendo incluir:

1.1.35.1.11.1. Classificação dos eventos de segurança;

1.1.35.1.11.2. Total de eventos avaliados;

1.1.35.1.11.3. Total de eventos escalados;

1.1.35.1.11.4. TOP aplicações mais impactadas, TOP origens dos eventos de segurança;

1.1.35.1.11.5. TOP endereços de destino das ameaças;

1.1.35.1.11.6. TOP URLs e suas categorias;

1.1.35.1.11.7. TOP atacantes, vulnerabilidades, ameaças, alarmes, violações de auditoria;

1.1.35.1.11.8. Principais tipos de ataques;

1.1.35.1.11.9. Descrição dos casos de uso utilizados para avaliar os alertas de segurança;

1.1.35.1.11.10. Novas informações de inteligência configuradas na ferramenta: como as novas regras de monitoramento, dashboards, assinaturas instaladas, etc;

1.1.35.1.12. O Sistema de Ticket ofertado deverá ser utilizado para registrar e escalar eventos de segurança, de modo a permitir o registro, envio de notificações e alertas entre as equipes do CONTRATANTE e da própria CONTRATADA;

1.1.35.1.13. O CONTRATANTE é responsável por avaliar os incidentes escalados após o processo de triagem inicial. Caso o incidente seja confirmado, o CONTRATANTE executará os seus processos e procedimentos internos para executar as medidas de contenção e correção, incluindo configurações nos sensores de segurança ou outros ativos. O CONTRATANTE registrará as ações realizadas no tíquete correspondente ao incidente, permitindo que a CONTRATADA esteja ciente do fechamento do mesmo;

1.1.35.1.14. Os analistas do CONTRATANTE responsáveis pelos tíquetes escalados devem possuir acesso total as informações do incidente relacionado;

1.1.35.1.15. Os analistas do CONTRATANTE devem poder contatar os analistas da CONTRATADA, por telefone ou via Sistema de Ticket, para consulta de informações em caso de qualquer dúvida sobre os eventos escalados e demais procedimentos para tratamento dos incidentes. As solicitações e respostas de informações adicionais sobre os incidentes, como logs e evidências, devem ser anexadas ao tíquete registrado na ferramenta;

1.1.35.1.16. O CONTRATANTE é responsável por fornecer informações de negócio adequadas, seguindo a regra do privilégio mínimo e necessidade de conhecer, para melhoria da atividade de monitoramento da CONTRATADA;

1.1.35.1.17. O CONTRATANTE pode solicitar, a qualquer momento, a customização dos indicadores e informações sobre incidentes e eventos apresentados nos relatórios. A CONTRATADA deve avaliar os requisitos técnicos necessários e operacionalizar. As solicitações devem ser registradas e realizadas por meio dos canais de suporte da CONTRATADA;

1.1.35.1.18. Por padrão, a CONTRATADA não deve possuir nenhum tipo de acesso aos ativos, sensores e ferramentas de proteção do CONTRATANTE. Em casos específicos e por tempo determinado, caso autorizado pela área de segurança do CONTRATANTE, pode ser fornecido acesso de leitura de registros do IPS, dados de sessão de rede (flow) e outras ferramentas de segurança para auxiliar em pesquisas pontuais de eventos de se gurança. Não será fornecido nenhum tipo de acesso a dados ou sistemas do CONTRATANTE, além dos estritamente necessários para o serviço de monitoramento que serão armazenados na ferramenta de inteligência;

1.1.35.1.19. A CONTRATADA deve prover informação específica sobre ameaças, gerada através de um processo (com coleta, validação, correlação, avaliação e interpretação de conhecimento baseado em evidências), que colocam em perigo ativos de informação ou de tecnologia do CONTRATANTE. Tal inteligência pode ser usada para embasar decisões sobre a resposta a tal ameaça ou risco, permitindo melhorar as táticas de detecção de ataques e configuração dos sensores de segurança. O processo deve resultar ainda em conhecimento utilizado para criação de novos indicadores e auxiliar na detecção de ataques futuros, possibilitando a identificação de ameaças específicas ao ambiente do CONTRATANTE;

1.1.35.2. CARACTERÍSTICAS E REQUISITOS INDISPENSÁVEIS PARA OS SERVIÇOS E RECURSOS FORNECIDOS PELO SECURITY OPERATIONS CENTER (SOC):

1.1.35.2.1. CORRELACIONAMENTO DE EVENTOS DE SEGURANÇA DA INFORMAÇÃO

1.1.35.2.1.1. Todo o gerenciamento dos componentes e funções administrativas devem ser feitas através de uma única interface web, acessível por navegador, sem a necessidade de instalação de aplicação adicionais;

1.1.35.2.1.2. A solução deverá ser fornecida para instalação e uso no idioma Português Brasil e Inglês;

1.1.35.2.1.3. A solução deverá ter o pleno funcionamento independentemente de conexão (física ou lógica) com o fabricante;

1.1.35.2.1.4. A solução deve sincronizar o horário de seus componentes utilizando o serviço NTP;

1.1.35.2.1.5. A solução deve ser gerenciada centralmente (configurações, controle e atualizações), através de interface web única, sem necessidades de intervenção nos equipamentos onde está instalado;

1.1.35.2.1.6. A solução deve ser licenciada com a capacidade de coletar, processar e correlacionar 200 (duzentos) eventos por segundo de forma sustentada. Deve-se considerar os eventos com tamanho médio de 700 bytes;

1.1.35.2.1.7. A solução deve permitir a recepção de eventos que excedam temporariamente os limites contrata dos, processando o volume excedente assim que volume for normalizado. Mantendo a operação com situações de picos temporários, sem incorrer na perda de eventos e sem incorrer em: qualquer cobrança adicional por excesso ou bloqueio da solução;

1.1.35.2.1.8. A comunicação entre os componentes da solução deverá ser feita de forma criptografada, garantindo a autenticidade, confidencialidade e integridade dos dados;

1.1.35.2.1.9. Para o acesso à interface web de administração, deve permitir o uso de certificado digital emitido por autoridade certificado interna da organização ou por autoridade certificadora reconhecida pelos navegadores;

1.1.35.2.1.10. Ter suporte a monitoração por SNMPv2c e SNMPv3;

1.1.35.2.1.11. A administração da solução deve usar uma única conta para cada usuário administrador (mesma conta, mesma senha), independente da funcionalidade gerenciada;

1.1.35.2.1.12. A coleta, normalização e o correlacionamento dos eventos provenientes dos

dispositivos monitorados devem ser realizadas próximos ao tempo real;

1.1.35.2.1.13. Os eventos devem ser normalizados e categorizados em um padrão único que será usado pela solução;

1.1.35.2.1.14. Deve permitir a definição de metadados customizados/personalizados, para extrair dados existentes na linha de log (raw), usando recursos como expressões regulares ou algum recurso gráfico para essa extração;

1.1.35.2.1.15. Propriedades customizadas devem poder ser usadas em regras de correlação online e em regras de correlação histórica;

1.1.35.2.1.16. Permitir a agregação de eventos semelhantes;

1.1.35.2.1.17. Deve atribuir métrica de prioridade para os eventos e para os alertas/incidentes;

1.1.35.2.1.18. Gerar alertas/incidentes com base nas regras definidas previamente;

1.1.35.2.1.19. Verificar conformidade com as políticas, controles e normas internas (customizadas) e regulamentações externas (ex. ISO 27001);

1.1.35.2.1.20. Deve permitir armazenar os eventos, inclusive os normalizados, de forma compactada;

1.1.35.2.1.21. Apresentar painéis gráficos (dashboards) com indicativos de situações relacionados à segurança, compliance, aplicações e monitoração do próprio sistema;

1.1.35.2.1.22. Os painéis gráficos (dashboards) devem ser customizáveis, por usuário;

1.1.35.2.1.23. Permitir a análise de eventos baseados em contexto, tais como, usuários, localização geográfica, bem como qualquer outro metadado contido no evento;

1.1.35.2.1.24. Enviar notificações relacionadas a um incidente/alerta por e-mail, trap snmp e syslog;

1.1.35.2.1.25. A solução deverá ter, no mínimo, as seguintes formas de coleta de eventos: Syslog (UDP, TCP), Syslog criptografado com TLS, JDBC, SNMP (v1, v2 e v3), Microsoft Event Log, MQ Series client, Arquivos de Log em formato de texto, Kafka, AWS Cloudwatch, Checkpoint OPSEC/LEA, CISCO NSEL e Juniper NSM Pro tocol;

1.1.35.2.1.26. Deve permitir a configuração de ofuscação de qualquer parte dos dados recebidos, assim que normalizados;

1.1.35.2.1.27. A ofuscação de dados deve ser configurada com chaves de criptografia;

1.1.35.2.1.28. Possuir a capacidade de automatizar a resposta a incidentes, através da execução de scripts, como ação customizada dentro das regras de correlação;

1.1.35.2.1.29. Tratar eventos em formato "comprimido" (zip, gz, tar.gz), sem a necessidade da descompressão manual;

1.1.35.2.1.30. Deverá fazer a agregação de eventos, mostrando a contagem de eventos, quando o mesmo evento ocorrer dentro de um período curto. A opção de realizar ou não a agregação de eventos deve ser configurável, por dispositivo integrado;

1.1.35.2.1.31. Deve manter o evento bruto ("raw") e seus metadados para o armazenamento e consulta futura;

1.1.35.2.1.32. Deve ser capaz de agregar informações sobre localização geográfica dos endereços IP envolvidos no evento, para que a mesma seja usada no correlacionamento;

1.1.35.2.1.33. A solução deve suportar, nativamente, pelo menos as seguintes fontes de logs: Windows, Linux, IBM/AIX, IBM/RACF, HPUX, Solaris, Oracle Database, IBM/DB2, MS SQL Server, Firewalls (Checkpoint, Cisco/ ASA, Juniper, Fortinet e Palo Alto e SonicWall), Network IPS (Sourcefire, IBM/ISS, HP Tipping Point, Snort e McAfee);

1.1.35.2.1.34. A solução deve suportar "overlap de IP", isto é, rotular os eventos para que seja possível gerenciar eventos de fontes de log que estejam em redes diferentes, mas possuem o mesmo endereçamento IP;

1.1.35.2.1.35. Deve exibir perfil visual do tráfego em tempo real, e normalizada de forma agregada. Deve incluir informações de bytes, pacotes e protocolos;

1.1.35.2.1.36. Usar mecanismo de correlação para a detecção de ataques de negação de serviço (DoS) e de negação de serviço distribuído (DDoS) a partir dos flows de rede;

1.1.35.2.1.37. Deve possuir mecanismo para não sofrer as consequências da monitoração de flows de rede em uma situação de DDoS;

1.1.35.2.1.38. Deve suportar o recebimento dos seguintes protocolos de flow: Netflow (versão 5 e 9), IPFIX, J Flow, sFlow (versões 2, 4 e 5) e Packeteer;

1.1.35.2.1.39. Monitorar a rede e identificar padrão de tráfego que possa ser uma ameaça, bem como detectar tráfego de rede de aplicativos como compartilhamento de arquivos, P2P e jogos;

1.1.35.2.1.40. Deve ser capaz de apresentar informações de fluxo de rede por período de tempo pré-definido;

1.1.35.2.1.41. Deve ser capaz de montar visualizações de fluxo de rede baseados em comunicações provenientes ou destinadas à internet agrupado por regiões geográficas;

1.1.35.2.1.42. Deve correlacionar logs e flows em conjunto, gerando incidentes de segurança;

1.1.35.2.1.43. Deve possuir regras de correlação específicas para regulações/conformidades, com suporte no mínimo a: ISO 27001 e GDPR/LGPD;

1.1.35.2.1.44. Deve possuir repositório do fabricante da solução que ofereça novas regras de correlação especializada em segurança para atualização e ampliação da capacidade de detecção de incidentes, sem custo adicional;

1.1.35.2.1.45. Deve permitir a criação de regras que identifiquem mudanças de comportamento, como surto ou ausência de eventos/tráfego, quando comparados a outros períodos similares (ex. mesmo período do dia, mesmo dia da semana);

1.1.35.2.1.46. Capacidade de fazer o correlacionamento entre eventos e fluxos de rede, NetFlow, J-Flow, S-Flow e IPFIX, sem a necessidade de ferramentas de terceiros ou qualquer componente adicional ao licenciamento da solução;

1.1.35.2.1.47. Possuir pelo menos os seguintes tipos de correlação:

1.1.35.2.1.44.1. Correlação por regras;

1.1.35.2.1.44.2. Extrapolação de um limite (threashold);

1.1.35.2.1.44.3. Correlação por anomalia e padrão de comportamento;

1.1.35.2.1.48. Como resultado das regras, deve ser capaz de executar ações automáticas, no mínimo: enviar e mail, enviar mensagem para o usuário conectado no console, criar um incidente no sistema de workflow interno, enviar traps SNMP e popular lista (watch list);

1.1.35.2.1.49. Disponibilizar pelo menos uma base de inteligência em ameaças com informações de riscos globais, com updates diários, integrada às regras de correlação para detecção de incidentes;

1.1.35.2.1.50. Qualquer metadado dos eventos pode ser usado em uma regra de correlação;

1.1.35.2.1.51. A correlação histórica deve permitir a escolha do período a ser analisado, atendendo no mínimo a correlação compreendo a análise de 1 dia, 7 dias e 30 dias;

1.1.35.2.1.52. Mecanismo para ajuste fino de regras de correlação, exibindo de forma gráfica as regras de correlação que são mais acionadas por eventos (que geram mais alertas) e seus

elementos relacionados. Facilitando o refinamento da solução com vistas à redução de falso-positivo e melhoria da performance;

1.1.35.2.1.53. Identificação de ações que comprometam dados cobertos pelas regulações LGPD (Lei Geral de Proteção a Dados) ou GDPR (General Data Protection Regulation);

1.1.35.2.1.54. Comunicação dos equipamentos internos com sites conhecidos por serem controladores de botnet;

1.1.35.2.1.55. Deve permitir o uso de algoritmo para garantia de integridade dos eventos armazenados, utilizando no mínimo os algoritmos: MD2, MOS, SHA-256, SHA-384 e SHA-512;

1.1.35.2.1.56. Deve permitir o uso dos algoritmos para garantia de integridade, do item anterior, com código de autenticação da mensagem (HMAC);

1.1.35.2.1.57. Permitir a remoção de dados das listas (watchlist) de forma manual, automática através de regras de correlação, por API ReST e pela expiração do tempo de vida da informação;

1.1.35.2.1.58. A solução deve implementar auto monitoração, para detectar comandos que possam modificar arquivos de logs, tentativas de logins por força bruta, edição e remoção de arquivos sensíveis ou críticos da solução e o uso de contas compartilhadas de administradores da solução;

1.1.35.2.1.59. Possuir capacidade de integração com bases Microsoft Active Directory, LDAP, TACACS e RADIUS para autenticação de usuários;

1.1.35.2.1.60. Deve permitir a integração com Single Sign-On que suporte o protocolo SAML 2.0;

1.1.35.2.1.61. Permitir pesquisa nos eventos históricos, a partir de metadados, fornecendo capacidade de "drill down", ou seja, o refinamento da pesquisa a partir da seleção de elementos no resultado, para efetuar nova pesquisa;

1.1.35.2.1.62. Capacidade de criação de novos painéis gráficos (dashboards) e alteração dos existentes;

1.1.35.2.1.63. Permitir a criação de novos modelos de relatórios e alteração dos relatórios nativos da solução sem a necessidade de uso de linguagens de programação, através da interface web;

1.1.35.2.1.64. Permitir agendar a geração de relatórios de forma periódica e notificar/enviar automaticamente os relatórios gerados para os destinatários dos mesmos;

1.1.35.2.1.65. Deve possuir templates de relatórios para as principais normas de conformidade. Sendo exigido, no mínimo, o atendimento a IS0/27001;

1.1.35.2.1.66. Permitir a manipulação dos incidentes identificados pela solução usando a API ReST, permitindo adicionar anotações, identificar os detalhes do incidente e encerrar o incidente usando esse acesso;

1.1.35.2.1.67. Deve permitir a geração de relatórios, contendo múltiplas informações num mesmo relatório, como dados de segurança e rede;

1.1.35.2.1.68. Deve permitir a criação de relatórios relacionados a: incidentes, logs, flows de rede, vulnerabilidades;

1.1.35.2.1.69. Deve gerar relatórios de eventos, alertas/incidentes em nível técnico e gerencial os quais devem ter a possibilidade de serem gerados em PDF, HTML, XLS;

1.1.35.2.1.70. Deve possuir módulo capaz de extrair os dados de usuário e ações executadas dos eventos coleta dos para geração de score de risco;

1.1.35.2.1.71. Deve ser capaz de importar dados de usuário em bases LDAP, CSV e Windows AD para identificação da pessoa associada a conta do sistema monitorado, deve ser capaz de

coletar e associar no mínimo: nome completo, departamento, contas associadas, e-mail e cargo;

2. DAS CONDIÇÕES DE INSTALAÇÃO

2.1. É/será de inteira responsabilidade da CONTRATADA a correta instalação, configuração e funciona menta dos equipamentos e componentes da solução ofertada, caso um dos serviços de instalação (itens 22 a 28) seja contratado. Os equipamentos e componentes serão implementados pela CONTRATADA de acordo com os termos deste TR. Não serão admitidos configurações e ajustes que impliquem no funcionamento do equipamento ou componente de hardware fora das condições normais recomendadas pelo fabricante.

2.2. A instalação e configuração dos equipamentos será de responsabilidade da CONTRATANTE caso nenhum dos itens 22 a 28 seja contratado.

2.3. Em processos de implantação de Firewall de Aplicação Web Virtual ou Datacenter (itens 19 a 21), Firewall SEDE (itens 5 a 7), Firewall DATA CENTER (itens 8 a 10) ou mais de 10 unidades de Firewall UNIDADE REMOTA (itens 1 a 4) deverão ser realizadas as seguintes atividades:

2.4. Deverá ser realizada uma reunião de kick-off do projeto, nas instalações do CONTRATANTE, com a participação do gerente técnico do projeto, dos responsáveis comercial, de design da solução, pelo técnico responsável pela implementação do projeto;

2.5. O planejamento dos serviços de instalação deve resultar num documento tipo SOW (Scope of Work, em tradução livre, escopo de trabalho). Neste documento devem conter a relação, descrição e quantidades dos produtos fornecidos, descrição da infraestrutura atual e desejada, topologia do ambiente, detalhamento dos serviços que serão executados, premissas do projeto, locais e horários de execução dos serviços, condições de execução dos serviços, pontos de contato do CONTRATANTE e CONTRATADA, cronograma de execução do projeto em etapas, com responsáveis e data e início e fim (se aplicável), relação da documentação a ser entregue ao final da execução dos serviços, responsabilidade do CONTRATANTE e CONTRATADA, plano de gerenciamento de mudanças, itens excluídos no projeto e termo de aceite;

2.6. Todos os parâmetros a serem configurados deverão ser alinhados entre as partes em reuniões de pré- projeto, devendo a CONTRATADA sugerir as configurações de acordo com normas técnicas e boas práticas, cabendo à contratante a sua aceitação expressa ou recusa nos casos de não atendimento das condições estabelecidas;

2.7. Os serviços deverão ser realizados por pessoal técnico experiente e certificado pelo fabricante dos equipamentos. Em momento anterior à instalação, a contratante poderá solicitar os comprovantes da qualificação profissional do técnico que executará os serviços, sendo direito da mesma a sua aceitação ou exigência de troca de profissional no caso de este não satisfizer às condições supramencionadas;

2.8. Ao término dos serviços deve ser criado um relatório detalhado contendo todos os itens configura dos no projeto (relatório as-built), etapas de execução e toda informação pertinente para posterior continuidade e manutenção da solução instalada, como usuários e endereços de acesso, configurações realizadas e o resumo das configurações dos equipamentos. Este relatório deve ser enviado com todas as informações em até 15 (quinze) dias após a finalização dos serviços;

2.9. A CONTRATADA deverá fornecer documentação completa da solução, incluindo especificação do equipamento, características e funcionalidades implementadas, desenho lógico da implantação, comentários e configurações executadas. Deverá conter também todas as configurações executadas em equipamentos de terceiros, quando for o caso;

2.10. Em processos de implantação de até 10 unidades de Firewall UNIDADE REMOTA (itens 1 a 4) os processos detalhados em 5.3 podem ser executados de maneira simplificada sendo, no entanto, obrigatório:

2.11. Os serviços deverão ser realizados por pessoal técnico experiente e certificado pelo fabricante dos equipamentos. Em momento anterior à instalação, a contratante poderá solicitar os

comprovantes da qualificação profissional do técnico que executará os serviços, sendo direito da mesma a sua aceitação ou exigência de troca de profissional no caso de este não satisfizer às condições supramencionadas;

2.12. Relatório as-built simplificado;

2.13. Documentação completa da solução, incluindo especificação do equipamento, características e funcionalidades implementadas, comentários e configurações executadas.

___

ANEXO B - ESPECIFICAÇÕES DA SOLUÇÃO DE GERÊNCIA CENTRALIZADA E RELATORIA

1. Deve permitir o gerenciamento e administração centralizado, possibilitando o gerenciamento de diversos equipamentos de proteção de rede desde que não sejam software livre;

2. O módulo de gerência deve ser capaz de gerenciar e administrar as soluções dos itens 1 a 11 descritas neste termo;

3. Caso a solução possua licenciamento por número de equipamentos gerenciados, deve ser licenciada para o número necessário de equipamentos a serem gerenciados;

4. Caso a solução possua licenças relacionadas a armazenamento, deve ser ofertado a sua maior capacidade suportada ou ilimitada;

5. Caso a solução possua módulo de relatórios estendida, deve ser também entregue junto com a solução;

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

7. Centralizar a administração de regras e políticas dos equipamentos de proteção de rede, usando uma única interface de gerenciamento;

8. O gerenciamento da solução deve suportar acesso via SSH, cliente do próprio fabricante ou WEB (HTTPS);

9. O gerenciamento deve permitir/possuir monitoração de logs, ferramentas de investigação de logs e acesso concorrente de administradores.

10. Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

11. Suportar criação de regras que fiquem ativas em horário definido e suportar criação de regras com data de expiração;

12. Suportar backup das configurações e rollback de configuração para a última configuração salva;

13. Suportar validação de regras antes da aplicação;

14. Suportar validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);

15. Deve permitir a visualização dos logs de uma regra específica em tempo real e na mesma tela de configura ção da regra selecionada;

16. Deve possibilitar a integração com outras soluções de SIEM de mercado desde que não sejam software li vre;

17. Suportar geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;

18. Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e Anti Malware), etc;

19. Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus, Anti- Malware), e URLs que passaram pela solução;

20. Deve ser possível exportar os logs em CSV;

21. Deve possibilitar a geração de relatórios de eventos no formato PDF;

22. Possibilitar rotação do log;

23. Suportar geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:

24. Resumo gráfico de aplicações utilizadas, principais aplicações por utilização de largura de banda, principais aplicações por taxa de transferência de bytes, principais hosts por número de ameaças identificadas, atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus e Anti-Malware), de rede vinculadas a este tráfego;

25. Deve permitir a criação de relatórios personalizados;

26. Suportar enviar os relatórios de forma automática via PDF:

27. A solução de gerenciamento deverá ser entregue como appliance virtual e deve ser compatível/homologado para VMware ESXi versão 5 e superior.

28. Deve consolidar logs e relatórios de todos os dispositivos administrados;

29. Capacidade de definir administradores com diferentes perfis de acesso com, no mínimo, as permissões de Leitura/Escrita e somente Leitura;

30. Deverá possuir mecanismo de Drill-Down para navegação e análise dos logs em tempo real;

31. Nas opções de Drill-Down, deve ser possível identificar o usuário que fez determinado acesso;

32. Permitir que os relatórios possam ser salvos, enviados e impressos;Deve incluir uma ferramenta do próprio fabricante ou de outro, desde que não seja software livre, ou em composição com terceiros, para correlacionar os eventos de segurança das funcionalidades adquiridas de todos os equipamentos e softwares ofertados;

33. Deve permitir a criação de filtros com base em qualquer característica do evento, tais como a origem e o IP destino, serviço, tipo de evento, severidade do evento, nome do ataque, o país de origem e destino etc.;

34. A solução deve prover, no mínimo, as seguintes funcionalidades para análise avançada dos incidentes:

35. Visualizar quantidade de tráfego utilizado de aplicações e navegação;

36. Gráficos com principais eventos de segurança de acordo com a funcionalidade selecionada;

37. A solução de correlação deve possuir mecanismo para detectar login de administradores em horários irregu lares;

38. A solução deve ser capaz de detectar ataques de tentativa de login e senha utilizando tipos diferentes de credencias;

39. Deve suportar a geração de relatório gerencial para apresentar aos executivos os eventos de ataque de for ma completamente visual, utilizando, para tanto, gráficos, consumo de banda utilizado pelos ataques e quanti dade de eventos gerados e protegidos;

40. Deve permitir a integração com servidores de autenticação LDAP Microsoft Aclive Directory e Radius;

41. Permitir criações de políticas de acesso de usuários autenticada no Active Directory, de forma que reconhe ça os usuários de forma transparente;

42. Permitir o download de assinaturas, atualizações e firmwares para distribuição centralizada aos dispositivos de segurança integrados a mesma;

43. Permitir a visualização de gráficos e mapa de ameaças;

44. Possuir mecanismo para que logs antigos sejam removidos automaticamente;

45. Deve permitir a criação de dashboards customizados para visibilidades do tráfego de aplicativos, categorias de URL, ameaças, serviços, países, origem e destino;

46. Deve possuir a capacidade de visualizar na interface gráfica da solução, informações do sistema como li cenças, memória, disco e uso de CPU;

47. A solução deve ser capaz de correlacionar eventos de todas as fontes de log em tempo real;

48. A solução deve fornecer conteúdo de correlação pré-definido organizado por categoria;

49. A solução deve possuir painéis de eventos em tempo real com possibilidade de configuração das atualiza ções e frequências;

ANEXO C - PLATAFORMA DE MONITORAMENTO

1. A Plataforma de Monitoramento deverá permitir a monitoração dos firewalls, a partir de um servidor central, possibilitando a geração de notificações específicas para cada equipe, através de acesso WEB à aplicação de gerenciamento com as seguintes características:

2. A interface de gerenciamento deverá ser em modo WEB acessada através de navegador.

3. Deverá ser compatível com, pelo menos, um dos seguintes navegadores: Google Chrome, Mozilla Firefox ou Internet E xplorar.

4. Permitir que as informações gerenciadas, coletadas em diversos pontos de captura, sejam consolidadas em uma única visão em um console gráfico central.

5. Possuir a capacidade de reiniciar serviços de monitoração automaticamente após a ocorrência de "queda" e alertar em sequência o retorno do equipamento que está sendo gerenciado.

6. Deverá ter capacidade de monitoração dos equipamentos ofertados neste edital em, pelo menos, os seguin tes itens:

6.1. Modelo do equipamento;

6.2. Utilização de CPU;

6.3. Uso de memória RAM;

6.4. Espaço livre em disco;

6.5. Versão do sistema operacional;

6.6. Status ou data de expiração do licenciamento;

6.7. Temperatura de operação do equipamento;

6.8. Status da (s) fonte (s) de alimentação;

6.9. Número de conexões ou sessões concorrentes;

6.10. Lista de interfaces de rede, contemplando, também:

6.10.1. Status das interfaces;

6.10.2. Throughput das interfaces;

6.10.3. Status da funcionalidade de alta disponibilidade;

7. Gatilhos e alertas:

7.1. A plataforma deve permitir a construção para a detecção de eventos (gatilhos) de acordo com a necessidade de gerenciamento dos sistemas, gerando os alertas necessários. Como exemplo, ela deve permitir a criação de gatilhos quando limites forem excedidos. Os alertas devem ser configuráveis para criação de SLAs. Os alertas devem ser visualizados também pela interface gráfica.

7.2. O envio de E-mail e SMS devem ser configurados por tipo de alerta em cada recurso monitorado, permitindo, por exemplo, que em diferentes interfaces de um mesmo equipamento existam gatilhos e formas de envios diferentes.

7.3. Prover o envio de alarmes para a console de gerenciamento de aplicações e E-mails e SMS para os Administradores quando os recursos monitorados atingirem os seus respectivos gatilhos.

7.4. Para o mesmo item podem ser gerados vários gatilhos com criticidade diferentes, permitindo assim, um melhor controle do tipo de problema.

8. Possuir processo de coleta que não necessite a instalação de agentes nos equipamentos monitorados;

9. Deve suportar o monitoramento através do protocolo SNMP nas versões 1, 2c e 3 e SNMP Traps;

10. Análise, relatórios e comparação:

10.1. Armazenar informações para posterior análise, que possa permitir comparações para acertos nos equipamentos.

10.2. A solução deverá possuir uma interface interna para geração de relatórios.

10.3. A solução deve possuir interface WEB para geração e visualização de relatórios.

10.4. A interface WEB deve possibilitar o envio de relatórios por E-mail manualmente ou mesmo préagendar a geração e o envio em uma data ou horários especificados.

10.5. A solução deve possibilitar a exportação dos relatórios em pelo menos dois dos seguintes formatos:

10.5.1. PDF.

10.5.2. HTML.

10.5.3. csv.

10.6. Todos os relatórios devem ter a flexibilidade de exibir informações em tempo real e também dados históricos, coletados em períodos anteriores.

10.7. A solução deve permitir a publicação automática de relatórios no formato HTML em um servidor WEB, permitindo uma análise sobre a situação dos servidores monitorados, com as seguintes características:

10.7.1. Apresentação dos nomes dos equipamentos no relatório.

10.7.2. Apresentação das informações gerenciadas por equipamento.

10.7.3. Exibição por grupo de equipamentos previamente estabelecidos.

10.8. Opções de periodicidade especificada pelo usuário: diária, semanal, mensal, trimestral, anual ou intervalo de data.

11. Apresentação em modo gráfico:

11.1. Dependência entre objetos monitorados: permitir que sejam cadastradas dependências entre os objetos monitorados, inclusive no nível de subitem de monitoramento, permitindo analisar o impacto de uma pa rada perante os demais objetos monitorados;

ANEXO D – ÓRGÃOS PARTICIPANTES DA ATA

Órgão/Entidade	ENDEREÇO
ETICE	Av. Pontes Vieira, 220 - São João do Tauape, Fortaleza - CE, 60130-240

ANEXO E – COMPROVAÇÃO DAS ESPECIFICAÇÕES TÉCNICAS

1. Este Anexo deve ser preenchido pelo Licitante com a descrição detalhada das características técnicas dos itens cotados, que possibilitem uma completa avaliação dos mesmos.

2. Este anexo é de preenchimento obrigatório pelo Licitante, sendo motivo de desclassificação do certame o seu não preenchimento;

3. O preenchimento deste Anexo deverá ser realizado baseado em documentos cuja origem seja exclusivamente do fabricante dos equipamentos, como catálogos, manuais, ficha de especificação técnica, informações obtidas em sites oficiais do fabricante através da Internet, indicando as respectivas URL (Uniform Resource Locator), ou por meio de declarações do fabricante. As comprovações devem ser claras, com indicação de página na proposta ou documento. A não comprovação de alguma característica exigida no Termo de Referência levará à desclassificação da proposta;

4. Os documentos utilizados para comprovação das especificações técnicas como folders, manuais e catálogos deverão ser entregues preferencialmente em formato PDF;

5. A comprovação técnica é exigida para todos os itens descritos no item **1.1, ESPECIFICAÇÃO DETALHADA** do **ANEXO A – ESPECIFICAÇÕES DETALHADAS**, assim como no **ANEXO B - ESPECIFICAÇÕES DA SOLUÇÃO DE GERÊNCIA CENTRALIZADA E RELATORIA** e no **ANEXO C - PLATAFORMA DE MONITORAMENTO**.

6. A documentação técnica deverá apresentar, ainda, em local de fácil reconhecimento, a identificação da data de emissão e da versão do produto a que se refere.

7. A tabela ilustrativa abaixo exemplifica como as Comprovações Técnicas deverão ser apresentadas:

Descrição	Link/ Documento	Página	Tópico
1.1.1. ITEM 1 NEXT GENERATION FIREWALL UNIDADE TIPO 1	--------	--------	
1.1.1.1. CARACTERÍSTICAS GERAIS	--------	--------	
1.1.1.1.1. É permitida a composição da solução ofertada entre diversos fabricantes, desde que não contemple solução de software livre;	Arquivo "b"	2	xxxx
1.1.1.1.2. A solução deverá ser compatível com SNMPv2 e SNMPv3;	Arquivo "x"	4	xxxx
……...			
…….			
1. 1.1.35.2.1.70. Deve possuir módulo capaz de extrair os	Arquivo "y"	1	xxxx

dados de usuário e ações executadas dos eventos coleta dos para geração de score de risco;			
1.1.35.2.1.71. Deve ser capaz de importar dados de usuário em bases LDAP, CSV e Windows AD para identificação da pessoa associada a conta do sistema monitorado, deve ser capaz de coletar e associar no mínimo: nome completo, departamento, contas associadas, e-mail e cargo;	Arquivo "z"	3	xxxx

ANEXO II - CARTA PROPOSTA

À

Central de Licitações do Estado do Ceará

Ref.: Pregão Eletrônico nº **20240008**

A proposta encontra-se em conformidade com as informações previstas no edital e seus anexos.

1. Identificação do licitante:

1. Razão Social:

2. CPF/CNPJ e Inscrição Estadual:

3. Endereço completo:

4. Representante Legal (nome, nacionalidade, estado civil, profissão, RG, CPF, domicílio):

5. Telefone, celular, fax, e-mail:

2. Condições Gerais da Proposta:

- A presente proposta é válida por _____ (_____) dias, contados da data de sua emissão.
- O objeto contratual terá garantia de _____(_____) _____.

3. Formação do Preço

GRUPO/ITEM _____						
ITEM	ESPECIFICAÇÃO	MARCA	UNIDADE DE FORNECIMENTO	QUANTIDADE	VALOR UNITÁRIO (R$)	VALOR TOTAL (R$)
VALOR GLOBAL R$ Valor por extenso (_____)						

DECLARO, sob as sanções administrativas cabíveis, inclusive as criminais e sob as penas da lei, que toda documentação anexada ao sistema é autêntica.

Local e data

Assinatura do representante legal

(Nome e cargo)

ANEXO III – MINUTA DA ATA DE REGISTRO DE PREÇOS

Ata de Registro de Preços nº ___ /20__

Pregão Eletrônico nº **20240008**

Processo Nº **30032.000154/2024-71**

Aos __ dias do mês de _____ de 20__, na sede da_____, foi lavrada a presente Ata de Registro de Preços, conforme deliberação da Ata do Pregão Eletrônico nº **20240008** do respectivo resultado homologado, publicado no Diário Oficial do Estado em __/__/20__, às fls ____, do processo nº_____, que vai assinada pelo titular do(a) _____, gestor(a) do Registro de Preços, pelos representantes legais dos detentores do registro de preços, todos qualificados e relacionados ao final, a qual será regida pelas cláusulas e condições seguintes:

1. DO OBJETO

1.1. Registro de preços para futuras e eventuais aquisições de solução de proteção de redes, incluindo aquisições de hardware e software e respectivo serviço de implantação, posterior monitoramento e suporte técnico 24x7x365, contemplando utilização de equipamentos obrigatoriedade todos novos e de primeiro uso, encontram-se detalhados no Anexo I – Termo de Referência do edital de Pregão Eletrônico nº **20240008** que passa a fazer parte desta Ata, com as propostas de preços apresentadas pelos detentores de preços registrados classificados em primeiro lugar, conforme consta nos autos do Processo nº **30032.000154/2024-71**.

1.2. Este instrumento não obriga a Administração a firmar contratações, exclusivamente por seu intermédio, podendo realizar licitações específicas, obedecida a legislação pertinente, sem que, desse fato, caiba recurso ou indenização de qualquer espécie aos detentores do registro de preços, sendo-lhes assegurado a preferência, em igualdade de condições.

2. DA FUNDAMENTAÇÃO LEGAL

2.1. O presente instrumento fundamenta-se:

I- No Pregão Eletrônico nº **20240008**

II- Nos termos do Decreto Estadual nº 35.323, de 24/02/2023, publicado D.O.E de 28/02/2023 e suas alterações.

III- Na Lei Federal nº 14.133, de 1º de abril de 2021.

3. DA ENTIDADE GERENCIADORA E DOS PARTICIPANTES

3.1. Compete ao órgão ou entidade gerenciadora desta Ata, o controle e a administração do sistema de registro de preços, em especial o contido no art. 17 do Decreto nº 35.323/2023.

3.2. O órgão ou entidade gerenciadora desta Ata será a EMPRESA DE TECNOLOGIA DA INFORMAÇÃO DO CEARÁ – ETICE.

3.3. Os órgãos e entidades participantes desta ata de registro de preços poderão realizar

contratações decorrentes de remanejamento de quantitativos ou valores cedidos por outros participantes, mediante autorização por meio de ferramenta informatizada, disponibilizada pela Seplag, desde que limitadas ao objeto licitado.

3.4. Aos órgãos e entidades participantes, competem observar o contido no art. 18 do mesmo decreto de que trata o subitem 3.1 acima.

4. DA ADESÃO À ATA DE REGISTRO DE PREÇOS

4.1. Durante a vigência desta ata, os órgãos ou entidades do Poder Executivo estadual participantes desta ou na condição de interessados, poderão realizar contratações decorrentes de remanejamento de quantitativo ou valores cedidos por outros participantes, mediante autorização prévia do órgão ou entidade gerenciadora, dispensada a elaboração do ETP.

4.1.1. Caso o remanejamento seja para execução de serviço em município diferente do estabelecido no edital, caberá ao beneficiário da ata de registro de preços, observadas as condições nela fixadas, optar pela aceitação ou não do remanejamento dos itens.

4.1.2. Os órgãos e entidades do Poder Executivo estadual e de outros entes federativos, não participantes desta ata de registro de preços, poderão realizar contratações decorrentes desta, na condição de interessados sem remanejamento, mediante autorização prévia do órgão ou entidade gerenciadora e do detentor do preço registrado.

4.1.2.1. A faculdade conferida de que trata este subitem estará limitada a órgãos e entidades da Administração Pública estadual, distrital e municipal que, na condição de não participantes, desejarem aderir à ata de registro de preços de órgão ou entidade gerenciadora do Poder Executivo estadual.

4.1.3. A adesão a ata observará os seguintes requisitos:

I- Apresentação de justificativa da vantagem da adesão;

II- Demonstração de que os valores registrados estão compatíveis com os valores praticados pelo mercado na forma do art. 23 da Lei nº 14.133/2021; e

III- Consulta e aceitação prévias do órgão ou da entidade gerenciadora e do detentor do preço registrado.

4.1.3.1. A autorização do órgão ou entidade gerenciadora apenas será realizada após a aceitação da adesão do detentor do preço registrado.

4.1.3.2. A entidade gerenciadora poderá rejeitar adesões caso elas possam acarretar prejuízo à execução de seus próprios contratos ou à sua capacidade de gerenciamento.

4.1.3.3. As aquisições ou contratações adicionais não poderão exceder, por órgão ou entidade, a 50% (cinquenta por cento) do total dos quantitativos dos itens registrados para o órgão gerenciador e para os órgãos participantes.

4.1.3.4. O quantitativo decorrente das adesões à ata de registro de preços a que se refere o subitem anterior não poderá exceder, na totalidade, ao dobro do quantitativo de cada item registrado na ata de registro de preços para o órgão gerenciador e órgãos participantes, independentemente do número de órgãos não participantes que aderirem.

4.1.4. O órgão ou entidade não participante deverá efetivar a aquisição ou contratação solicitada em até 90 (noventa) dias, contados a partir da autorização do órgão ou entidade gerenciadora, observado o prazo de vigência da ata.

5. DA VALIDADE DA ATA, DA FORMALIZAÇÃO DO CONTRATO E DO CADASTRO RESERVA

5.1. O prazo de vigência da ata de registro de preços será de 1 (um) ano, contado a partir da data da sua publicação no Diário Oficial do Estado, e poderá ser prorrogado, por igual período, desde que por acordo entre as partes e comprovado o preço vantajoso, nas mesmas condições e quantidades ou valores remanescentes.

5.2. É vedado efetuar acréscimos nos quantitativos ou valores fixados pela ata de registro de preços, inclusive o acréscimo de que trata o art. 125 da Lei nº 14.133/2021.

5.3. O prazo de vigência do contrato decorrente desta ata de registro de preços encontra-se definido no Termo de Referência, admitindo-se a prorrogação na forma da Lei, desde que a autoridade competente ateste que as condições e os preços permanecem vantajosos para a Administração, permitida a negociação com o contratado.

5.3.1. O instrumento contratual deverá ser assinado no prazo de vigência desta ata e passará a ter eficácia com a sua publicação no Diário Oficial do Estado.

5.3.2. Na formalização do contrato ou do instrumento equivalente deverá haver a indicação da disponibilidade dos créditos orçamentários respectivos.

5.4. Os contratos decorrentes desta ata de registro de preços poderão ser alterados, observado o disposto no § 4º do art. 15 do Decreto nº 35.323/2023.

5.5. Após a homologação da licitação, o licitante mais bem classificado, será convocado para assinar a ata de registro de preços, no prazo e nas condições estabelecidos no edital de licitação, sob pena de decair o direito, sem prejuízo das sanções previstas no edital e na Lei nº 14.133/2021.

5.5.1. O prazo de convocação poderá ser prorrogado 1 (uma) vez, por igual período, mediante solicitação do licitante convocado, desde que apresentada dentro do prazo, devidamente justificada, e que a justificativa seja aceita pela Administração.

5.5.2. A ata de registro de preços poderá ser assinada por certificação digital.

5.5.3. Serão observadas ainda as seguintes condições para a formalização da ata de registro de preços:

I- Serão registrados na ata os preços e os quantitativos do adjudicatário, que oferecer na proposta o quantitativo máximo estabelecido no Termo de Referência.

II- Será incluído na ata, na forma do anexo único, o registro dos licitantes que:

a) Aceitarem cotar os serviços com preços iguais aos do adjudicatário, observada a classificação da licitação, que comporão o cadastro de reserva; e

b) Mantiverem sua proposta original.

III- Será obedecida nas contratações a ordem de classificação dos licitantes registrados na ata.

a) O registro tem por objetivo a formação de cadastro de reserva para o caso de impossibilidade de atendimento pelo signatário da ata.

b) Para fins da ordem de classificação, os licitantes que aceitarem reduzir suas propostas para o preço do adjudicatário antecederão aqueles que mantiverem sua proposta original.

5.6. A convocação dos licitantes do cadastro de reserva ocorrerá quando o licitante vencedor não assinar a ata de registro de preços no prazo e nas condições estabelecidas no edital, ou na hipótese do cancelamento do preço registrado na forma do art. 25 do Decreto nº 35.323/2021.

5.6.1. A habilitação dos licitantes do cadastro reserva somente será realizada quando caracterizada a necessidade da contratação.

5.7. O preço registrado com indicação dos licitantes será divulgado no Diário Oficial do Estado. e ficará disponibilizado durante a vigência da ata de registro de preços.

5.8. Na hipótese da inexistência do cadastro de reserva, a Administração, observados o valor estimado e sua eventual atualização nos termos do edital, poderá:

I- Convocar para negociação os demais licitantes remanescentes cujos preços foram registrados sem redução, observada a ordem de classificação, com vistas à obtenção de preço melhor,

mesmo que acima do preço do adjudicatário; ou

II- Adjudicar e firmar o contrato nas condições ofertadas pelos licitantes remanescentes, atendida a ordem classificatória, quando frustrada a negociação de melhor condição.

5.9. A existência de preços registrados implicará compromisso do detentor do preço para a contratação, nas condições estabelecidas, mas não obrigará a Administração a contratar, facultada a realização de licitação específica para a demanda pretendida, desde que devidamente justificada.

6. DA ALTERAÇÃO OU ATUALIZAÇÃO DOS PREÇOS REGISTRADOS, DA NEGOCIAÇÃO, DA SUBSTITUIÇÃO DA MARCA OU MODELO E DA ALTERAÇÃO DE DADOS CONSTITUTIVOS DO DETENTOR DE PREÇOS.

6.1. Os preços registrados serão fixos e irreajustáveis durante a vigência da ata, exceto em decorrência das disposições contidas no art. 23 do Decreto nº 35.323/2023.

6.1.1. Os preços registrados são os preços unitários ofertados nas propostas dos detentores de preços, os quais estão relacionados no anexo único desta ata e servirão de base para futuras contratações, observadas as condições de mercado.

6.1.2. Os preços registrados poderão ainda ser alterados ou atualizados em caso de criação, alteração ou extinção de quaisquer tributos ou encargos legais ou a superveniência de disposições legais, com comprovada repercussão sobre os preços registrados;

6.2. Na hipótese de o preço registrado tornar-se superior ao preço praticado no mercado por motivo superveniente, o órgão ou entidade gerenciadora convocará o fornecedor para negociar a redução do preço registrado.

6.3. Caso não aceite reduzir seu preço aos valores praticados pelo mercado, o detentor do preço registrado será liberado do compromisso assumido quanto ao item registrado, sem aplicação de penalidades administrativas. Nesta hipótese, o gerenciador convocará os detentores de preços do cadastro de reserva ou, se não houver, os remanescentes que atenderem os termos do disposto nos §§ 3º, 5º e 6º do art. 12 do Decreto nº 35.323/2023, na ordem de classificação, para assegurar igual oportunidade de negociação..

6.3.1. Não havendo êxito nas negociações, o órgão ou entidade gerenciadora procederá ao cancelamento dos itens registrados, ou se for o caso, da Ata de registro de preços, adotando as medidas cabíveis para obtenção de contratação mais vantajosa.

6.4. Caso haja alteração do preço registrado, o órgão ou entidade gerenciadora comunicará o fato aos órgãos ou entidades participantes.

6.4.1. A alteração do preço registrado não altera automaticamente o preço do contrato decorrente da ata de registro de preços, cuja revisão deverá ser feita pelo órgão ou entidade contratante, observadas as disposições legais incidentes sobre o contrato.

6.5. O detentor do registro de preços poderá solicitar à entidade gerenciadora:

I - Substituição da marca ou modelo do item registrado por outra equivalente ou de qualidade superior, mantendo o mesmo preço e as mesmas especificações, desde que comprovada a inviabilidade do fornecimento da marca ou modelo originalmente registrado e que permaneça vantajosidade para a Administração;

II - Alteração da razão social ou outro dado constitutivo, mediante apresentação de termo aditivo ao documento de constituição da empresa.

6.5.1. No caso de deferimento às solicitações, a entidade gerenciadora fará a alteração na ata e comunicará aos órgãos ou entidades participantes para alteração do contrato.

7. DO CANCELAMENTO DO REGISTRO DE PREÇOS

7.1. O registro de preços será cancelado nas hipóteses previstas no art. 25 do Decreto nº

35.323/2023.

7.2. O cancelamento de preço registrado, será formalizado por despacho da autoridade competente do órgão ou entidade gerenciadora, assegurado o direito à ampla defesa e ao contraditório, e sua comunicação será feita por escrito, juntando-se a cópia nos autos que deram origem ao registro de preços.

7.3. No caso de ser ignorado, incerto ou inacessível o endereço do detentor do preço registrado, a comunicação será feita mediante publicação no Diário Oficial do Estado (DOE), considerando-se cancelado o preço registrado a partir da data da publicação.

7.4. Antes de cancelar o item ou revogar a ata, o órgão ou entidade gerenciadora deverá tomar providências no sentido de que não haja descontinuidade na prestação dos serviços.

7.5. Não sendo conveniente realizar novo processo de registro de preços, o órgão ou entidade gerenciadora deverá apresentar aos órgãos ou entidades participantes as justificativas que motivaram a não realização do mesmo e orientar sobre as ações para o novo processo de contratação.

8. DAS PENALIDADES

8.1. Compete ao órgão ou entidade gerenciadora, aplicar, garantida a ampla defesa e o contraditório, as penalidades decorrentes do descumprimento do pactuado nesta ata de registro de preços, nos processos que impliquem em impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar, conforme disposto no inciso IV do art. 17 do Decreto nº 35.323/2023, sem prejuízo das sanções legais nas esferas civil e criminal.

8.2. As sanções previstas no subitem anterior, serão aplicadas ao adjudicatário que injustificadamente se recusar assinar a ata de registro de preços, caracterizando-se o descumprimento total das obrigações assumidas. Aplica-se as mesmas sanções, aos integrantes do cadastro de reserva no registro de preços e os remanescentes com preços registrados.

8.3. O detentor de preço registrado recolherá a multa por meio de Documento de Arrecadação Estadual (DAE), ou se for o caso, por meio de depósito bancário podendo ser substituído por outro instrumento legal, em nome da contratante, se não o fizer, será cobrada em processo de execução.

9. DAS DISPOSIÇÕES GERAIS

9.1. As condições gerais da contratação, tais como o prazo para entrega e recebimento do objeto, obrigações do contratante e contratado, condições de pagamento, penalidades e demais condições do contrato, encontram-se definidas no Termo de Referência e Minuta do Contrato.

9.2. No caso de adjudicação por preço global de grupo de itens, só será admitida a contratação de parte de itens do grupo se houver prévia pesquisa de mercado e demonstração de sua vantagem para o órgão ou a entidade, conforme §6º do art. 20 do Decreto nº 35.323/2023.

10. DO FORO

Fica eleito o foro do município da contratante, para conhecer das questões relacionadas com a presente Ata que não possam ser resolvidas pelos meios administrativos.

Assinam esta Ata, os signatários relacionados e qualificados a seguir, os quais firmam o compromisso de zelar pelo fiel cumprimento das suas cláusulas e condições.

Signatários:

Órgão ou Entidade Gerenciadora da Ata.	Nome Titular	Cargo	CPF	RG	Assinatura

Detentores Adjudicatários do Reg. de Preços	Nome do Representante	Cargo	CPF	RG	Assinatura

Para firmeza e validade do pactuado, a presente Ata foi lavrada em ___ (____) vias de igual teor, que, depois de lida e achada em ordem, vai assinada pelas partes e encaminhada cópia aos órgãos e entidades participantes, se houver.

Fortaleza/CE, ___ de _____ de 20___

ANEXO ÚNICO DA ATA DE REGISTRO DE PREÇOS Nº ___ /20__ – MAPA DE PREÇOS DOS BENS E SERVIÇOS

Este documento é parte da Ata de Registro de Preços acima referenciada, celebrada entre o órgão ou entidade gerenciadora da ata e os prestadores de serviço, cujos preços estão a seguir registrados por item, em face da realização do Pregão Eletrônico nº **20240008**, seguido da relação do órgãos e entidades participantes.

Constam ainda registrados os preços dos prestadores de serviço que aceitaram cotar os itens com preços iguais ao adjudicatário e os que mantiveram sua proposta original:

Relação dos prestadores de serviço adjudicatários.

Item	Cód Item	Especificação do Item (se for o caso, incluir prazo de garantia)	Fornecedores	Unid	Quant. Máx	Quant. Min.	Preço Registrado

Relação dos Órgãos e Entidades Participantes da Ata.

Seq	Órgão/Entidade	ENDEREÇO

Relação de prestadores de serviço, segundo a ordem de classificação, que aceitaram cotar os itens com preços iguais ao adjudicatário(Cadastro Reserva).

Item	Cód Item	Especificação do Item (se for o caso, incluir prazo de garantia)	Fornecedores	Unid	Quant. Máx	Quant. Min.	Preço Registrado

Relação de prestadores de serviço, segundo a ordem de classificação, que mantiveram sua proposta original (Remanescentes):

Item	Cód Item	Especificação do Item (se for o caso, incluir prazo de garantia)	Fornecedores	Unid	Quant. Máx	Quant. Min.	Preço Registrado

ANEXO IV A – MINUTA DO TERMO DE CONTRATO (MODELO ADMINISTRAÇÃO DIRETA)

Contrato nº ___ / 20__ –

Processo nº _____

CONTRATO QUE ENTRE SI CELEBRAM (O)A_____E (O) A _____, ABAIXO QUALIFICADOS, PARA O FIM QUE NELE SE DECLARA.

O(A_____, situada(o) na _____, inscrita(o) no CNPJ sob o nº _____, doravante denominada(o) CONTRATANTE, neste ato representada(o) pelo _____, (nacionalidade), portador da Carteira de Identidade nº _____, e do CPF nº _____, residente e domiciliada(o) em (Município - UF), na _____, e a _____, com sede na _____, CEP: _____, Fone: _____, inscrita no CPF/CNPJ sob o nº _____, doravante denominado CONTRATADO, representado neste ato pelo _____, (nacionalidade), portador da Carteira de Identidade nº _____, e do CPF nº _____, residente e domiciliada(o) em (Município - UF), na _____, têm entre si justa e acordada a celebração do presente contrato, mediante as cláusulas e condições seguintes:

CLÁUSULA PRIMEIRA – DA FUNDAMENTAÇÃO

1.1. O presente contrato tem como fundamento o Pregão Eletrônico n° **20240008**, e seus anexos, os preceitos do direito público, Lei Federal nº 14.133, de 1º de abril de 2021, e demais legislação aplicável ao cumprimento de seu objeto.

CLÁUSULA SEGUNDA – DA VINCULAÇÃO AO EDITAL E A PROPOSTA

2.1. O cumprimento deste contrato está vinculado aos termos do edital do Pregão Eletrônico nº **20240008**, o Termo de Referência, a proposta do contratado e eventuais anexos dos respectivos documentos os quais constituem parte deste instrumento, independente de sua transcrição.

CLÁUSULA TERCEIRA – DO OBJETO

3.1. Registro de preços para futuras e eventuais aquisições de solução de proteção de redes, incluindo aquisições de hardware e software e respectivo serviço de implantação, posterior monitoramento e suporte técnico 24x7x365, contemplando utilização de equipamentos obrigatoriamente todos novos e de primeiro uso, nas condições estabelecidas neste contrato e no Termo de Referência do edital e na proposta do CONTRATADO.

CLÁUSULA QUARTA – DA VIGÊNCIA E PRORROGAÇÃO

4.1. O prazo de vigência do contrato é de 36 (trinta e seis) meses, contado da sua assinatura, na forma do art. 94 c/c o art. 105 da Lei Federal n° 14.133/2021, admitindo-se a prorrogação desde que a autoridade competente ateste que as condições e os preços permanecem vantajosos para a Administração, permitida a negociação com o CONTRATADO.

CLÁUSULA QUINTA – DO FORNECIMENTO

5.1. A forma de fornecimento, assim como os prazos e condições de conclusão, entrega, recebimento do objeto, obrigações e demais condições constam no Termo de Referência, anexo a este contrato.

CLÁUSULA SEXTA – DA SUBCONTRATAÇÃO

6.1. Será admitida a subcontratação do objeto contratual nos termos estabelecidos no subitem 21.7 do edital.

CLÁUSULA SÉTIMA – DO PREÇO

7.1. O valor total da contratação é de R$ _____ (_____)

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

CLÁUSULA OITAVA – DO PAGAMENTO E DO RECEBIMENTO

8.1. O prazo para pagamento ao CONTRATADO e demais condições a ele referentes, bem como, as condições de recebimento, se encontram definidos no Termo de Referência, anexo a este instrumento de contrato.

CLÁUSULA NONA – DO REAJUSTE

9.1. Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data do orçamento estimado, ou seja, a data da pesquisa constante no Mapa Comparativo de Preços.

9.2. Após o interregno de um ano, os preços iniciais poderão ser reajustados, mediante a aplicação, do índice IPCA, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

9.3. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

9.4. No caso de atraso ou não divulgação do(s) índice (s) de reajustamento, o CONTRATANTE pagará ao CONTRATADO a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).

9.5. Nas aferições finais, o(s) índice(s) utilizado(s) para reajuste será(ão), obrigatoriamente, o(s) definitivo(s).

9.6. Caso o(s) índice(s) estabelecido(s) para reajustamento venha(m) a ser extinto(s) ou de qualquer forma não possa(m) mais ser utilizado(s), será(ão) adotado(s), em substituição, o(s) que vier(em) a ser determinado(s) pela legislação então em vigor.

9.7. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

9.8. O reajuste será realizado por apostilamento.

CLÁUSULA DÉCIMA – DAS OBRIGAÇÕES DO CONTRATANTE E DO CONTRATADO

10.1. As obrigações referentes ao CONTRATANTE e ao CONTRATADO encontram-se, respectivamente, definidas no Termo de Referência, parte integrante deste termo.

CLÁUSULA DÉCIMA PRIMEIRA – DAS OBRIGAÇÕES PERTINENTES À LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

11.1. O CONTRATADO declara que tem ciência da existência da LGPD e se compromete a adequar todos os procedimentos internos ao disposto na legislação, com o intuito de proteger os dados pessoais que lhe forem repassados, cumprindo, a todo momento, as normas de proteção de dados pessoais, jamais colocando, por seus atos ou por sua omissão, o CONTRATANTE em situação de violação de tais regras.

11.1.1. O CONTRATADO somente poderá tratar dados pessoais nos limites e finalidades exclusivas do cumprimento de suas obrigações com base no presente contrato e jamais poderá realizar o tratamento para fins distintos da execução dos serviços especificados no certame ou no contrato administrativo.

11.2. O tratamento de dados pessoais será realizado de acordo com as hipóteses de tratamento previstas nos arts. 7º, 11, 14, 23, 24 e 26 da LGPD e somente para propósitos legítimos,

específicos, explícitos e informados ao titular, observando a persecução do interesse público e os princípios do art. 6º da LGPD e 37 da Constituição Federal de 1988.

11.3. O CONTRATADO deverá indicar, no prazo máximo de 5 (cinco) dias úteis da publicação do Aditivo, a identidade e informações de contato do seu Encarregado de Proteção de Dados, bem como, se aplicável, o endereço da página eletrônica onde essa designação é realizada, conforme estabelecido no § 1º do art. 41 da LGPD e se compromete a manter o CONTRATANTE informado sobre os dados atualizados de contato de seu Encarregado de Tratamento de Dados Pessoais, sempre que for substituído, independentemente das alterações em sua página eletrônica.

11.4. O CONTRATADO deverá cooperar com a Administração Direta e Indireta do Estado do Ceará no cumprimento das obrigações referentes ao exercício dos direitos dos Titulares previstos na LGPD e nas Leis e Regulamentos de Proteção de Dados em vigor e também no atendimento de requisições e determinações do Poder Judiciário, Ministério Público e Órgãos de Controle, quando relacionados ao objeto contratual.

11.5. O CONTRATADO não poderá disponibilizar ou transmitir a terceiros, sem prévia autorização por escrito, informação, dados pessoais ou base de dados a que tenha acesso em razão do cumprimento do objeto deste instrumento contratual.

11.5.1. Caso autorizada transmissão de dados pelo CONTRATADO a terceiros, as informações fornecidas e/ou compartilhadas devem se limitar ao estritamente necessário para o fiel desempenho da execução do instrumento contratual, adotando procedimentos de segurança que assegurem a sua confidencialidade, integridade e disponibilidade dos dados.

11.5.2. As PARTES se obrigam a zelar pelo sigilo dos dados, garantindo que apenas as pessoas que efetivamente precisam acessá-los o façam, submetendo-as, em todo caso, ao dever de confidencialidade.

11.6. Ocorrendo o término do tratamento dos dados nos termos do art. 15 da LGPD é dever do CONTRATADO eliminá-los, com exceção das hipóteses do art. 16 da mesma lei, incluindo aquelas em que houver necessidade de guarda de documentação para fins de comprovação do cumprimento de obrigações legais ou contratuais e somente enquanto não prescritas essas obrigações.

11.6.1. O CONTRATADO não poderá deter cópias ou backups, informações, dados pessoais e/ou base de dados a que tenha tido acesso durante a execução do cumprimento do objeto deste instrumento contratual.

11.6.2. O CONTRATADO deverá eliminar os dados pessoais a que tiver conhecimento ou posse em razão do cumprimento do objeto deste instrumento contratual tão logo não haja necessidade de seu tratamento.

11.6.3. O CONTRATADO fica obrigado a devolver todos os documentos, registros e cópias que contenham informação, dados pessoais, e/ou base de dados a que tenha tido acesso durante a execução do cumprimento do objeto deste instrumento contratual, no prazo de 30 (trinta) dias corridos, contados da data de qualquer uma das hipóteses de extinção do contrato, restando autorizada a conservação apenas nas hipóteses legalmente previstas,

11.7. Caso as PARTES necessitem subcontratar atividades relacionadas ao certame/contrato em que haja tratamento dos dados, deverão exigir a vinculação do SUBCONTRATADO (suboperador) aos critérios definidos neste instrumento, fazendo-o assinar um termo de adesão ao presente contrato.

11.7.1. O CONTRATANTE deverá ser informado no prazo de 5 (cinco) dias úteis sobre todos os contratos de subcontratação (suboperadores) firmados ou que venham a ser celebrados pelo CONTRATADO.

11.7.2. Em caso de subcontratação, o CONTRATADO e o SUBCONTRATADO responderão em regime de solidariedade por eventuais danos causados aos titulares, o CONTRATANTE e a

terceiros, em virtude de qualquer conduta comissiva ou omissiva inerente ao tratamento dos dados.

11.7.3. O CONTRATADO deverá assegurar que o subcontratado oferecerá o mesmo nível de segurança dos dados, produzindo e guardando evidências disso;

11.8. As PARTES devem adotar boas práticas de governança e medidas técnicas e administrativas em relação ao tratamento dos dados, compatíveis com a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados.

11.8.1. É dever do CONTRATADO orientar e treinar seus empregados sobre os deveres, requisitos e responsabilidades decorrentes da LGPD, inclusive dará conhecimento formal aos seus empregados das obrigações e condições acordadas nesta cláusula.

11.8.2. O CONTRATADO se responsabilizará por assegurar que todos os seus colaboradores, consultores, e/ou prestadores de serviços que, no exercício das suas atividades, tenham acesso e/ou conhecimento da informação e/ou dos dados pessoais, agirão de acordo com o presente contrato, com as leis de proteção de dados e que estes respeitem o dever de proteção, confidencialidade e sigilo, devendo estes assumir compromisso formal de preservar a confidencialidade e segurança de tais dados, documento que estar disponível em caráter permanente para exibição do CONTRATANTE, mediante solicitação.

11.8.3. O CONTRATADO deverá promover a revogação de todos os privilégios de acesso aos sistemas, informações e recursos do CONTRATANTE, em caso de desligamento de funcionário das atividades inerentes à execução do presente Contrato.

11.9. Em caso de incidente de segurança em relação aos dados tratados neste certame/contrato, que comprometa a confidencialidade, a integridade e a disponibilidade dos dados, a PARTE que sofreu o incidente deverá comunicar imediatamente a ocorrência a partir de uma notificação que conterá, no mínimo:

a) Data e hora do incidente;

b) Data e hora da ciência pela PARTE responsável;

c) Descrição dos dados pessoais afetados;

d) Número de titulares afetados;

e) Relação dos titulares envolvidos;

f) Riscos relacionados ao incidente;

g) Indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados;

h) Motivos da demora, no caso de a comunicação não haver sido imediata;

i) Medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo;

j) O contato do Encarregado de Proteção de Dados ou de outra pessoa junto a qual seja possível obter maiores informações sobre o ocorrido;

11.9.1. Na hipótese descrita acima, as PARTES atuarão em regime de cooperação para:

a) Definir e implementar as medidas necessárias para fazer cessar o incidente e minimizar seus impactos;

b) Prover as informações necessárias à apuração do ocorrido no menor prazo possível;

c) Definir o padrão de respostas a serem dadas aos titulares, terceiros, à ANPD e demais autoridades competentes.

11.10. Os dados obtidos em razão deste contrato serão armazenados em um banco de dados seguro, com garantia de registro das transações realizadas na aplicação de acesso (log), adequado controle baseado em função (role based access control) e com transparente

identificação do perfil dos credenciados, tudo estabelecido como forma de garantir inclusive a rastreabilidade de cada transação e a franca apuração, a qualquer momento, de desvios e falhas, vedado o compartilhamento dessas informações com terceiros;

11.11. A critério do CONTRATANTE, o CONTRATADO poderá ser provocado a colaborar na elaboração do Relatório de Impacto à Proteção de Dados Pessoais, conforme a sensibilidade e o risco inerente dos serviços objeto deste contrato, no tocante a dados pessoais.

11.12. O CONTRATADO indenizará o CONTRATANTE, em razão do não cumprimento das obrigações previstas nas leis, normas, regulamentos e recomendações das autoridades de proteção de dados com relação ao presente contrato, de quaisquer danos, prejuízos, custos e despesas, incluindo-se honorários advocatícios, multas, penalidades e eventuais dispêndios investigativos relativos a demandas administrativas ou judiciais propostas em face do CONTRATANTE a esse título.

11.13. Em caso de responsabilização do Estado por danos e/ou violações à LGPD decorrentes do objeto do contrato, deverá ser apurado os danos que efetivamente cada uma das partes causarem ao titular dos dados, para fins de assegurar o direito de regresso do Estado nos termos da legislação.

11.13.1. O CONTRATANTE poderá realizar diligência para aferir o cumprimento dessa cláusula, devendo o Contratado atender prontamente eventuais pedidos de comprovação formulados.

11.14. Os contratos e convênios de que trata o *§ 1º do art. 26 da Lei nº 13.709*/2018 deverão ser comunicados à ANPD.

11.15. Este instrumento pode ser alterado nos procedimentos pertinentes ao tratamento de dados pessoais, quando indicado pela autoridade competente, em especial a ANPD por meio de opiniões técnicas ou recomendações, editadas na forma da LGPD.

CLÁUSULA DÉCIMA SEGUNDA – DA GARANTIA DE EXECUÇÃO

12.1. A contratação conta com garantia de execução, nos moldes do art. 96 da Lei nº 14.133/2021, em valor correspondente a 5% (cinco por cento) do valor contratual, que deverá ser prestada até 10 (dez) dias úteis a contar da assinatura deste instrumento.

12.2. A apólice do seguro-garantia deverá acompanhar as modificações referentes à vigência do contrato principal mediante a emissão do respectivo endosso pela seguradora.

12.3. Será permitida a substituição da apólice de seguro-garantia na data de renovação ou de aniversário, desde que mantidas as condições e coberturas da apólice vigente e nenhum período fique descoberto, ressalvado o disposto no subitem 12.5, deste instrumento de contrato.

12.4. A garantia somente será liberada ou restituída após a fiel execução do contrato ou após a sua extinção por culpa exclusiva da Administração e, quando em dinheiro, será atualizada monetariamente.

12.5. Na hipótese de suspensão do contrato por ordem ou inadimplemento da Administração, o CONTRATADO ficará desobrigado de renovar a garantia ou de endossar a apólice de seguro até a ordem de reinício da execução ou o adimplemento pela Administração.

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

12.6.1. Prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;

12.6.2. Multas moratórias e punitivas aplicadas pela Administração ao CONTRATADO; e

12.6.3. Obrigações trabalhistas e previdenciárias de qualquer natureza e para com o FGTS, não adimplidas pelo CONTRATADO, quando couber.

12.7. A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados no subitem 12.6 , observada a legislação que rege a matéria.

12.8. A garantia em dinheiro deverá ser efetuada em favor do CONTRATANTE, em conta específica no Banco Bradesco S.A., com correção monetária.

12.9. Caso a opção seja por utilizar títulos da dívida pública, estes devem ter sido emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil, e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Economia.

12.10. No caso de garantia na modalidade de fiança bancária, deverá ser emitida por banco ou instituição financeira devidamente autorizada a operar no País pelo Banco Central do Brasil, e deverá constar expressa renúncia do fiador aos benefícios do art. 827 do Código Civil.

12.11. No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser ajustada ou renovada, seguindo os mesmos parâmetros utilizados quando da contratação.

12.12. Se o valor da garantia for utilizado total ou parcialmente em pagamento de qualquer obrigação, o CONTRATADO obriga-se a fazer a respectiva reposição no prazo máximo de _____ (_____) dias úteis, contados da data em que for notificada.

12.13. O CONTRATANTE executará a garantia na forma prevista na legislação que rege a matéria.

12.14. O emitente da garantia ofertada pelo CONTRATADO deverá ser notificado pelo CONTRATANTE quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais.

12.15. Caso se trate da modalidade seguro-garantia, ocorrido o sinistro durante a vigência da apólice, sua caracterização e comunicação poderão ocorrer fora desta vigência, não caracterizando fato que justifique a negativa do sinistro, desde que respeitados os prazos prescricionais aplicados ao contrato de seguro, nos termos do art. 20 da Circular Susep nº 662, de 11 de abril de 2022.

12.16. Extinguir-se-á a garantia com a restituição da apólice, carta fiança ou autorização para a liberação de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração do CONTRATANTE, mediante termo circunstanciado, de que o CONTRATADO cumpriu todas as cláusulas do contrato.

12.17. O garantidor não é parte para figurar em processo administrativo instaurado pelo CONTRATANTE com o objetivo de apurar prejuízos e/ou aplicar sanções ao CONTRATADO.

12.18. O CONTRATADO autoriza o CONTRATANTE a reter, a qualquer tempo, a garantia, na forma prevista neste contrato.

12.19. Além da garantia de que tratam os arts. 96 e seguintes da Lei nº 14.133/2021, a presente contratação possui previsão de garantia do serviço a ser fornecido, incluindo manutenção e assistência técnica, conforme o caso e condições estabelecidas no Termo de Referência.

CLÁUSULA DÉCIMA TERCEIRA – DAS INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

13.1. Comete infração administrativa, nos termos da Lei nº 14.133/2021, o CONTRATADO que :

13.1.1. Der causa à inexecução parcial do contrato;

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

13.1.3. Der causa à inexecução total do contrato;

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

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

13.1.6. Praticar ato fraudulento na execução do contrato;

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

13.1.8. Praticar ato lesivo previsto no art. 5º da Lei nº 12.846/2013.

13.2. Serão aplicadas ao CONTRATADO que incorrer nas infrações acima descritas as seguintes sanções:

13.2.1. Advertência, quando o CONTRATADO der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave;

13.2.2. Impedimento de licitar e contratar, quando praticadas as condutas descritas nos subitens 13.1.2, 13.1.3 e 13.1.4, deste contrato, sempre que não se justificar a imposição de penalidade mais grave;

13.2.3. Declaração de inidoneidade para licitar e contratar, quando praticadas as condutas descritas nos subitens 13.1.5, 13.1.6, 13.1.7 e 13.1.8 deste contrato, bem como nos subitens 13.1.2,13.1.3 e 13.1.4, que justifiquem a imposição de penalidade mais grave.

13.2.4. Multa:

13.2.4.1. Moratória de 0,2% (dois décimos por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 25 (vinte e cinco) dias.

13.2.4.2. Moratória de 0,07% (sete centésimos por cento) por dia de atraso injustificado sobre o valor total do contrato, até o máximo de 2% (dois por cento) pela inobservância do prazo fixado para apresentação, suplementação ou reposição da garantia.

13.2.4.2.1. O atraso superior a 30 (trinta) dias autoriza a Administração a promover a extinção do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõe o inciso I do art. 137 da Lei n. 14.133/2021.

13.2.4.3. Compensatória de 20% (vinte por cento) sobre o valor total do contrato, no caso de inexecução total do objeto.

13.3. A aplicação das sanções previstas neste contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao CONTRATANTE.

13.4. Todas as sanções previstas neste contrato poderão ser aplicadas cumulativamente com a multa.

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

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

13.6. Na aplicação das sanções serão considerados:

13.6.1. A natureza e a gravidade da infração cometida;

13.6.2. As peculiaridades do caso concreto;

13.6.3. As circunstâncias agravantes ou atenuantes;

13.6.4. Os danos que dela provierem para o CONTRATANTE;

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

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

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

13.9. O CONTRATANTE deverá, no prazo máximo 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ele aplicados, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no Cadastro Nacional de Empresas Punidas (Cnep), instituídos no âmbito do Poder Executivo Federal e no Certificado de Registro Cadastral(CRC) do Estado do Ceará.

13.10. As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133/2021.

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

13.11.1. Na impossibilidade do pagamento da multa por meio de descontos dos créditos existentes ou da garantia contratual, o CONTRATADO recolherá a multa por meio de Documento de Arrecadação Estadual (DAE), podendo ser substituído por outro instrumento legal, em nome do CONTRATANTE, se não o fizer, será cobrada em processo de execução.

CLÁUSULA DÉCIMA QUARTA – DA EXTINÇÃO CONTRATUAL

14.1. Este contrato se extingue nas seguintes hipóteses:

I- Quando cumpridas as obrigações de ambas as partes, ainda que isso ocorra antes do prazo estipulado para tanto, e.

II- Quando mesmo não cumpridas as obrigações nele estipuladas, ou antes do prazo nele fixado, ocorrer algum dos motivos previstos no art. 137 da Lei nº 14.133/2021, bem como amigavelmente, assegurados o contraditório e a ampla defesa.

a) Na hipótese do inciso II, aplicam-se também os arts. 138 e 139 da mesma Lei.

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

14.2.1. Se a operação implicar mudança da pessoa jurídica CONTRATADA, deverá ser formalizado termo aditivo para alteração subjetiva.

14.3. O termo de rescisão, sempre que possível, será precedido:

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

14.3.2. Relação dos pagamentos já efetuados e ainda devidos;

14.3.3. Indenizações e multas.

14.4. A extinção do contrato não configura óbice para o reconhecimento do desequilíbrio econômico-financeiro, hipótese em que será concedida indenização por meio de termo indenizatório.

14.5. Este contrato poderá ser rescindido a qualquer tempo pelo CONTRATANTE, mediante aviso prévio de no mínimo 30 (trinta) dias, nos casos das rescisões decorrentes do previsto no inciso VIII, do art. 137, da Lei Federal nº 14.133/2021, sem que caiba ao CONTRATADO, direito à indenização de qualquer espécie.

CLÁUSULA DÉCIMA QUINTA – DA DOTAÇÃO ORÇAMENTÁRIA

15.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Geral do Estado deste exercício, na dotação abaixo discriminada, conforme o caso:

15.1.1. Gestão/Unidade:

15.1.2. Fonte de Recursos:

15.1.3. Programa de Trabalho:

15.1.4. Elemento de Despesa:

15.1.5. Nota de Empenho:

15.2. A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

CLÁUSULA DÉCIMA SEXTA – DAS ALTERAÇÕES

16.1. Eventuais alterações contratuais reger-se-ão pela disciplina dos arts. 124 e seguintes da Lei nº 14.133/2021.

16.2. O CONTRATADO é obrigado a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

16.3. Registros que não caracterizam alteração do contrato podem ser realizados por simples apostila, dispensada a celebração de termo aditivo, na forma do art. 136 da Lei nº 14.133/2021.

CLÁUSULA DÉCIMA SÉTIMA – DOS CASOS OMISSOS

17.1. Os casos omissos serão decididos pelo CONTRATANTE, segundo as disposições contidas na Lei nº 14.133/2021, e demais normas estaduais aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078/1990 – Código de Defesa do Consumidor – e normas e princípios gerais dos contratos.

CLÁUSULA DÉCIMA OITAVA – DA PUBLICAÇÃO

18.1. Incumbirá ao CONTRATANTE divulgar o presente instrumento no Portal Nacional de Contratações Públicas (PNCP), na forma prevista no art. 94 da Lei 14.133/2021, bem como no respectivo sítio oficial na Internet, em atenção a Lei nº 12.527/2011, regulamentada no Estado do Ceará pela Lei nº 15.175/2012.

CLÁUSULA DÉCIMA NONA – DO FORO

19.1. Fica eleito o foro do município da sede do CONTRATANTE, para dirimir os litígios que decorrerem da execução deste Termo de Contrato que não puderem ser compostos pela conciliação, conforme art. 92, §1º, da Lei nº 14.133/2021.

E, por estarem de acordo, foi mandado lavrar o presente contrato, que está visado pela Assessoria Jurídica do CONTRATANTE, e do qual se extraíram 3 (três) vias de igual teor e forma, para um só efeito, as quais, depois de lidas e achadas conforme, vão assinadas pelos representantes das partes e pelas testemunhas abaixo.

Local e data

(nome do representante)
CONTRATANTE

(nome do representante)
CONTRATADO

Testemunhas:

(nome da testemunha 1)
RG:
CPF:

(nome da testemunha 2)
RG:
CPF:

Visto:

(nome do(a) procurador(a)/assessor(a) jurídico(a) da CONTRATANTE)

ANEXO IV B – MINUTA DO TERMO DE CONTRATO (MODELO PARA ESTATAIS)

Contrato nº ___ / 20__ –

Processo nº _____

CONTRATO QUE ENTRE SI CELEBRAM (O)A_____E (O) A _____, ABAIXO QUALIFICADOS, PARA O FIM QUE NELE SE DECLARA.

O(A_____, situada(o) na _____, inscrita(o) no CNPJ sob o nº _____, doravante denominada(o) CONTRATANTE, neste ato representada(o) pelo _____, (nacionalidade), portador da Carteira de Identidade nº _____, e do CPF nº _____, residente e domiciliada(o) em (Município - UF), na _____, e a _____, com sede na _____, CEP: _____, Fone: _____, inscrita no CPF/CNPJ sob o nº _____, doravante denominado CONTRATADO, representado neste ato pelo _____, (nacionalidade), portador da Carteira de Identidade nº _____, e do CPF nº _____, residente e domiciliada(o) em (Município - UF), na _____, têm entre si justa e acordada a celebração do presente contrato, mediante as cláusulas e condições seguintes:

CLÁUSULA PRIMEIRA – DA FUNDAMENTAÇÃO

1.1. O presente contrato tem como fundamento o Pregão Eletrônico n° **20240008**, e seus anexos, os preceitos do direito público, Lei Federal nº 13.303, de 30 de junho de 2016, o Regulamento Interno de Licitações e Contratos e demais legislação aplicável ao cumprimento de seu objeto.

CLÁUSULA SEGUNDA – DA VINCULAÇÃO AO EDITAL E A PROPOSTA

2.1. O cumprimento deste contrato está vinculado aos termos do edital do Pregão Eletrônico nº **20240008**, o Termo de Referência, a proposta do contratado e eventuais anexos dos respectivos documentos os quais constituem parte deste instrumento, independente de sua transcrição.

CLÁUSULA TERCEIRA – DO OBJETO

3.1. Registro de preços para futuras e eventuais aquisições de solução de proteção de redes, incluindo aquisições de hardware e software e respectivo serviço de implantação, posterior monitoramento e suporte técnico 24x7x365, contemplando utilização de equipamentos obrigatoriamente todos novos e de primeiro uso, nas condições estabelecidas neste contrato e no Termo de Referência do edital e na proposta do CONTRATADO.

CLÁUSULA QUARTA – DA VIGÊNCIA E ALTERAÇÃO

4.1. O prazo de vigência do contrato é de 36 (trinta e seis) meses, contado da sua assinatura, na forma do disposto no art. 71 da Lei Federal n° 13.303/2016.

4.2. O contrato poderá ser alterado nos casos previstos nos arts. 72 e 81 da Lei Federal n° 13.303/2016 e conforme dispuser o Regulamento Interno de Licitações e Contratos do CONTRATANTE.

4.3. Registros que não caracterizam alteração do contrato podem ser realizados por simples apostila, dispensada a celebração de termo aditivo.

CLÁUSULA QUINTA – DA EXECUÇÃO CONTRATUAL

5.1. O regime da execução contratual, assim como os prazos e condições de conclusão, entrega, recebimento do objeto, obrigações e demais condições constam no Termo de Referência, anexo a este contrato.

CLÁUSULA SEXTA – DA SUBCONTRATAÇÃO

6.1. Será admitida a subcontratação do objeto contratual nos termos estabelecidos no subitem 21.7 do edital.

CLÁUSULA SÉTIMA – DO PREÇO

7.1. O valor total da contratação é de R$ _____ (_____)

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

CLÁUSULA OITAVA – DO PAGAMENTO E DO RECEBIMENTO

8.1. O prazo para pagamento ao CONTRATADO e demais condições a ele referentes, bem como, as condições de recebimento, encontram-se definidos no Termo de Referência, anexo a este instrumento de contrato.

CLÁUSULA NONA – DO REAJUSTE

9.1. Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data da apresentação da proposta.

9.2. Após o interregno de um ano, e independentemente de pedido do CONTRATADO, os preços iniciais serão reajustados, mediante a aplicação, pelo CONTRATANTE, do índice IPCA, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

9.3. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

9.4. No caso de atraso ou não divulgação do(s) índice (s) de reajustamento, o CONTRATANTE pagará ao CONTRATADO a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).

9.5. Nas aferições finais, o(s) índice(s) utilizado(s) para reajuste será(ão), obrigatoriamente, o(s) definitivo(s).

9.6. Caso o(s) índice(s) estabelecido(s) para reajustamento venha(m) a ser extinto(s) ou de qualquer forma não possa(m) mais ser utilizado(s), será(ão) adotado(s), em substituição, o(s) que vier(em) a ser determinado(s) pela legislação então em vigor.

9.7. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

9.8. O reajuste será realizado por apostilamento.

CLÁUSULA DÉCIMA – DAS OBRIGAÇÕES DO CONTRATANTE E DO CONTRATADO

10.1. As obrigações referentes ao CONTRATANTE e ao CONTRATADO encontram-se, respectivamente, definidas no Termo de Referência, parte integrante deste instrumento.

CLÁUSULA DÉCIMA PRIMEIRA – DAS OBRIGAÇÕES PERTINENTES À LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

11.1. O CONTRATADO declara que tem ciência da existência da LGPD e se compromete a adequar todos os procedimentos internos ao disposto na legislação, com o intuito de proteger os dados pessoais que lhe forem repassados, cumprindo, a todo momento, as normas de proteção de dados pessoais, jamais colocando, por seus atos ou por sua omissão, o CONTRATANTE em situação de violação de tais regras.

11.1.1. O CONTRATADO somente poderá tratar dados pessoais nos limites e finalidades exclusivas do cumprimento de suas obrigações com base no presente contrato e jamais poderá realizar o tratamento para fins distintos do fornecimento dos bens especificados no certame ou no contrato administrativo.

11.2. O tratamento de dados pessoais será realizado de acordo com as hipóteses de tratamento previstas nos artigos 7º, 11, 14, 23, 24 e 26 da LGPD e somente para propósitos legítimos, específicos, explícitos e informados ao titular, observando a persecução do interesse público e os princípios do art. 6º da LGPD e 37 da Constituição Federal de 1988.

11.3. O CONTRATADO deverá indicar, no prazo máximo de 5 (cinco) dias úteis da publicação do Aditivo, a identidade e informações de contato do seu Encarregado de Proteção de Dados, bem como, se aplicável, o endereço da página eletrônica onde essa designação é realizada, conforme estabelecido no § 1º do art. 41 da LGPD e se compromete a manter o CONTRATANTE informado sobre os dados atualizados de contato de seu Encarregado de Tratamento de Dados Pessoais, sempre que for substituído, independentemente das alterações em sua página eletrônica.

11.4. O CONTRATADO deverá cooperar com a Administração Direta e Indireta do Estado do Ceará no cumprimento das obrigações referentes ao exercício dos direitos dos Titulares previstos na LGPD e nas Leis e Regulamentos de Proteção de Dados em vigor e também no atendimento de requisições e determinações do Poder Judiciário, Ministério Público e Órgãos de Controle, quando relacionados ao objeto contratual.

11.5. O CONTRATADO não poderá disponibilizar ou transmitir a terceiros, sem prévia autorização por escrito, informação, dados pessoais ou base de dados a que tenha acesso em razão do cumprimento do objeto deste instrumento contratual.

11.5.1. Caso autorizada transmissão de dados pelo CONTRATADO a terceiros, as informações fornecidas e/ou compartilhadas devem se limitar ao estritamente necessário para o fiel desempenho da execução do instrumento contratual, adotando procedimentos de segurança que assegurem a sua confidencialidade, integridade e disponibilidade dos dados.

11.5.2. As PARTES se obrigam a zelar pelo sigilo dos dados, garantindo que apenas as pessoas que efetivamente precisam acessá-los o façam, submetendo-as, em todo caso, ao dever de confidencialidade.

11.6. Ocorrendo o término do tratamento dos dados nos termos do art. 15 da LGPD é dever do CONTRATADO eliminá-los, com exceção das hipóteses do art. 16 da mesma lei, incluindo aquelas em que houver necessidade de guarda de documentação para fins de comprovação do cumprimento de obrigações legais ou contratuais e somente enquanto não prescritas essas obrigações.

11.6.1. O CONTRATADO não poderá deter cópias ou backups, informações, dados pessoais e/ou base de dados a que tenha tido acesso durante a execução do cumprimento do objeto deste instrumento contratual.

11.6.2. O CONTRATADO deverá eliminar os dados pessoais a que tiver conhecimento ou posse em razão do cumprimento do objeto deste instrumento contratual tão logo não haja necessidade de seu tratamento.

11.6.3. O CONTRATADO fica obrigado a devolver todos os documentos, registros e cópias que contenham informação, dados pessoais, e/ou base de dados a que tenha tido acesso durante a execução do cumprimento do objeto deste instrumento contratual, no prazo de 30 (trinta) dias corridos, contados da data de qualquer uma das hipóteses de extinção do contrato, restando autorizada a conservação apenas nas hipóteses legalmente previstas,

11.7. Caso as PARTES necessitem subcontratar atividades relacionadas ao certame/contrato em que haja tratamento dos dados, deverão exigir a vinculação do SUBCONTRATADO (suboperador) aos critérios definidos neste instrumento, fazendo-o assinar um termo de adesão ao presente contrato.

11.7.1. O CONTRATANTE deverá ser informado no prazo de 5 (cinco) dias úteis sobre todos os contratos de subcontratação (suboperadores) firmados ou que venham a ser celebrados pelo CONTRATADO.

11.7.2. Em caso de subcontratação, o CONTRATADO e o SUBCONTRATADO responderão em regime de solidariedade por eventuais danos causados aos titulares, o CONTRATANTE e a terceiros, em virtude de qualquer conduta comissiva ou omissiva inerente ao tratamento dos dados.

11.7.3. O CONTRATADO deverá assegurar que o subcontratado oferecerá o mesmo nível de segurança dos dados, produzindo e guardando evidências disso;

11.8. As PARTES devem adotar boas práticas de governança e medidas técnicas e administrativas em relação ao tratamento dos dados, compatíveis com a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados.

11.8.1. É dever do CONTRATADO orientar e treinar seus empregados sobre os deveres, requisitos e responsabilidades decorrentes da LGPD, inclusive dará conhecimento formal aos seus empregados das obrigações e condições acordadas nesta cláusula.

11.8.2. O CONTRATADO se responsabilizará por assegurar que todos os seus colaboradores, consultores, e/ou prestadores de serviços que, no exercício das suas atividades, tenham acesso e/ou conhecimento da informação e/ou dos dados pessoais, agirão de acordo com o presente contrato, com as leis de proteção de dados e que estes respeitem o dever de proteção, confidencialidade e sigilo, devendo estes assumir compromisso formal de preservar a confidencialidade e segurança de tais dados, documento que estar disponível em caráter permanente para exibição do CONTRATANTE, mediante solicitação.

11.8.3. O CONTRATADO deverá promover a revogação de todos os privilégios de acesso aos sistemas, informações e recursos do CONTRATANTE, em caso de desligamento de funcionário das atividades inerentes à execução do presente Contrato.

11.9. Em caso de incidente de segurança em relação aos dados tratados neste certame/contrato, que comprometa a confidencialidade, a integridade e a disponibilidade dos dados, a PARTE que sofreu o incidente deverá comunicar imediatamente a ocorrência a partir de uma notificação que conterá, no mínimo:

a) Data e hora do incidente;

b) Data e hora da ciência pela PARTE responsável;

c) Descrição dos dados pessoais afetados;

d) Número de titulares afetados;

e) Relação dos titulares envolvidos;

f) Riscos relacionados ao incidente;

g) Indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados;

h) Motivos da demora, no caso de a comunicação não haver sido imediata;

i) Medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo;

j) O contato do Encarregado de Proteção de Dados ou de outra pessoa junto a qual seja possível obter maiores informações sobre o ocorrido;

11.9.1. Na hipótese descrita acima, as PARTES atuarão em regime de cooperação para:

a) Definir e implementar as medidas necessárias para fazer cessar o incidente e minimizar seus impactos;

b) Prover as informações necessárias à apuração do ocorrido no menor prazo possível;

c) Definir o padrão de respostas a serem dadas aos titulares, terceiros, à ANPD e demais autoridades competentes.

11.10. Os dados obtidos em razão deste contrato serão armazenados em um banco de dados seguro, com garantia de registro das transações realizadas na aplicação de acesso (log), adequado controle baseado em função (role based access control) e com transparente identificação do perfil dos credenciados, tudo estabelecido como forma de garantir inclusive a rastreabilidade de cada transação e a franca apuração, a qualquer momento, de desvios e falhas, vedado o compartilhamento dessas informações com terceiros;

11.11. A critério do CONTRATANTE, o CONTRATADO poderá ser provocado a colaborar na elaboração do Relatório de Impacto à Proteção de Dados Pessoais, conforme a sensibilidade e o risco inerente dos bens e/ou serviços objeto deste contrato, no tocante a dados pessoais.

11.12. O CONTRATADO indenizará o CONTRATANTE, em razão do não cumprimento por parte da CONTRATADA das obrigações previstas nas leis, normas, regulamentos e recomendações das autoridades de proteção de dados com relação ao presente contrato, de quaisquer danos, prejuízos, custos e despesas, incluindo-se honorários advocatícios, multas, penalidades e eventuais dispêndios investigativos relativos a demandas administrativas ou judiciais propostas em face do CONTRATANTE a esse título.

11.13. Em caso de responsabilização do Estado por danos e/ou violações à LGPD decorrentes do objeto do contrato, deverá ser apurado os danos que efetivamente cada uma das partes causarem ao titular dos dados, para fins de assegurar o direito de regresso do Estado nos termos da legislação.

11.13.1. O CONTRATANTE poderá realizar diligência para aferir o cumprimento dessa cláusula, devendo o Contratado atender prontamente eventuais pedidos de comprovação formulados.

11.14. Os contratos e convênios de que trata o § 1º do art. 26 da Lei nº 13.709/2018 deverão ser comunicados à ANPD.

11.15. Este instrumento pode ser alterado nos procedimentos pertinentes ao tratamento de dados pessoais, quando indicado pela autoridade competente, em especial a ANPD por meio de opiniões técnicas ou recomendações, editadas na forma da LGPD.

CLÁUSULA DÉCIMA SEGUNDA – DA GARANTIA DE EXECUÇÃO

12.1. A contratação conta com garantia de execução, nos moldes do art. 70 da Lei Federal nº 13.303/2021, em valor correspondente a ____% (____ por cento) do valor contratual, que deverá ser prestada até 10 (dez) dias úteis a contar da assinatura deste instrumento.

12.2. Em se tratando de seguro-garantia, a apólice deverá acompanhar as modificações referentes à vigência do contrato principal mediante a emissão do respectivo endosso pela seguradora.

12.3. Será permitida a substituição da apólice de seguro-garantia na data de renovação ou de aniversário, desde que mantidas as condições e coberturas da apólice vigente e nenhum período fique descoberto, ressalvado o disposto no subitem 12.5, deste instrumento de contrato.

12.4. A garantia somente será liberada ou restituída após a fiel execução do contrato ou após a sua extinção por culpa exclusiva da Administração e, quando em dinheiro, será atualizada monetariamente.

12.5. Na hipótese de suspensão do contrato por ordem ou inadimplemento da Administração, o CONTRATADO ficará desobrigado de renovar a garantia ou de endossar a apólice de seguro até a ordem de reinício da execução ou o adimplemento pela Administração.

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

12.6.1. Prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;

12.6.2. Multas moratórias e punitivas aplicadas pela Administração ao CONTRATADO; e

12.6.3. Obrigações trabalhistas e previdenciárias de qualquer natureza e para com o FGTS, não adimplidas pelo CONTRATADO, quando couber.

12.7. A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados no subitem 12.6, observada a legislação que rege a matéria.

12.8. A garantia em dinheiro deverá ser efetuada com correção monetária em favor do CONTRATANTE, em conta preferencialmente no Banco Bradesco S.A, ou outro banco indicado pelo contratante.

12.9. Caso a opção seja por utilizar títulos da dívida pública, estes devem ter sido emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil, e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Economia.

12.10. No caso de garantia na modalidade de fiança bancária, deverá ser emitida por banco ou instituição financeira devidamente autorizada a operar no País pelo Banco Central do Brasil, e deverá constar expressa renúncia do fiador aos benefícios do art. 827 do Código Civil.

12.11. No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser ajustada ou renovada, seguindo os mesmos parâmetros utilizados quando da contratação.

12.12. Se o valor da garantia for utilizado total ou parcialmente em pagamento de qualquer obrigação, o CONTRATADO obriga-se a fazer a respectiva reposição no prazo máximo de _____ (_____) dias úteis, contados da data em que for notificada.

12.13. O CONTRATANTE executará a garantia na forma prevista na legislação que rege a matéria.

12.14. O emitente da garantia ofertada pelo CONTRATADO deverá ser notificado pelo CONTRATANTE quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais.

12.15. Caso se trate da modalidade seguro-garantia, ocorrido o sinistro durante a vigência da apólice, sua caracterização e comunicação poderão ocorrer fora desta vigência, não caracterizando fato que justifique a negativa do sinistro, desde que respeitados os prazos prescricionais aplicados ao contrato de seguro, nos termos do art. 20 da Circular Susep nº 662, de 11 de abril de 2022.

12.16. Extinguir-se-á a garantia com a restituição da apólice, carta fiança ou autorização para a liberação de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração do CONTRATANTE, mediante termo circunstanciado, de que o CONTRATADO cumpriu todas as cláusulas do contrato.

12.17. O garantidor não é parte para figurar em processo administrativo instaurado pelo CONTRATANTE com o objetivo de apurar prejuízos e/ou aplicar sanções ao CONTRATADO.

12.18. O CONTRATADO autoriza o CONTRATANTE a reter, a qualquer tempo, a garantia, na forma prevista neste contrato.

12.19. Além da garantia de que trata o art. 70 da Lei nº 13.303/2016, a presente contratação possui previsão de garantia do serviço a ser fornecido, incluindo manutenção e assistência técnica, conforme o caso e condições estabelecidas no Termo de Referência.

CLÁUSULA DÉCIMA TERCEIRA – DAS INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

13.1. Pela inexecução total ou parcial do contrato a empresa pública ou a sociedade de economia mista poderá, garantida a prévia defesa, aplicar ao CONTRATADO as seguintes sanções:

I - advertência;

II - multa, na forma a seguir:

a. Moratória de 0,2% (dois centésimos por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 25 (vinte e cinco) dias.

b. Moratória de 0,07% (sete centésimos por cento) por dia de atraso injustificado sobre o valor total do contrato, até o máximo de 2% (dois por cento) pela inobservância do prazo fixado para apresentação, suplementação ou reposição da garantia.

c. O atraso superior a 30 (trinta) dias autoriza a Administração a promover a extinção do contrato por descumprimento ou cumprimento irregular de suas cláusulas.

d. Compensatória de 20% (vinte por cento) sobre o valor total do CONTRATADO, no caso de inexecução total do objeto.

III - suspensão temporária de participação em licitação e impedimento de contratar com a entidade sancionadora, por prazo não superior a 2 (dois) anos.

13.2. Se a multa aplicada for superior ao valor da garantia prestada, além da perda desta, responderá o CONTRATADO pela sua diferença, que será descontada dos pagamentos eventualmente devidos pela empresa pública ou pela sociedade de economia mista ou cobrada judicialmente.

13.3. As sanções previstas nos incisos I e III do subitem 13.1 poderão ser aplicadas juntamente com a do inciso II, devendo a defesa prévia do interessado, no respectivo processo, ser apresentada no prazo de 10 (dez) dias úteis.

13.4. As sanções previstas no inciso III subitem 13.1 poderão também ser aplicadas às empresas ou aos profissionais que, em razão dos contratos regidos por esta Lei:

I - tenham sofrido condenação definitiva por praticarem, por meios dolosos, fraude fiscal no recolhimento de quaisquer tributos;

II - tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;

III - demonstrem não possuir idoneidade para contratar com a empresa pública ou a sociedade de economia mista em virtude de atos ilícitos praticados.

13.5. Na impossibilidade do pagamento da multa por meio de descontos dos créditos existentes ou da garantia contratual, o CONTRATADO recolherá a multa por meio de depósito bancário podendo ser substituído por outro instrumento legal, em nome do contratante, se não o fizer, será cobrada em processo de execução.

CLÁUSULA DÉCIMA QUARTA – DA EXTINÇÃO CONTRATUAL

14.1. Este contrato poderá ser extinto nas hipóteses de inadimplemento contratual, acordo entre as partes, ou conforme dispuser regulamento interno do CONTRATANTE.

14.2. Este contrato poderá ser extinto a qualquer tempo pelo CONTRATANTE, mediante aviso prévio de no mínimo 30 (trinta) dias, nos casos das rescisões decorrentes de razões de interesse público, justificadas pela autoridade máxima da CONTRATANTE, sem que caiba ao CONTRATADO, direito à indenização de qualquer espécie.

CLÁUSULA DÉCIMA QUINTA – DOS RECURSOS ORÇAMENTÁRIOS

15.1. As despesas decorrentes da contratação serão provenientes dos recursos _____.

CLÁUSULA DÉCIMA SEXTA – DOS CASOS OMISSOS

16.1. Os casos omissos serão decididos pelo CONTRATANTE, segundo as disposições contidas na Lei nº 13.303/2016, Regulamentos Internos e demais normas estaduais aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078/1990 – Código de Defesa do Consumidor – e normas e princípios gerais dos contratos.

CLÁUSULA DÉCIMA SÉTIMA – DA PUBLICAÇÃO

17.1. Incumbirá ao CONTRATANTE divulgar a publicação resumida do presente instrumento nos termos do §2º do art. 51 da Lei nº 13.303/2016 e no Regulamento Interno de Licitações.

CLÁUSULA DÉCIMA OITAVA – DO FORO

18.1. Fica eleito o foro do município da sede do CONTRATANTE, para dirimir os litígios que decorrerem da execução deste Termo de Contrato que não puderem ser compostos pela conciliação.

E, por estarem de acordo, foi mandado lavrar o presente contrato, que está visado pela Assessoria Jurídica do CONTRATANTE, e do qual se extraíram 3 (três) vias de igual teor e forma, para um só efeito, as quais, depois de lidas e achadas conforme, vão assinadas pelos representantes das partes e pelas testemunhas abaixo.

Local e data

(nome do representante) (nome do representante)

CONTRATANTE CONTRATADO

Testemunhas:

(nome da testemunha 1) (nome da testemunha 2)

RG: RG:

CPF: CPF:

Visto:

(nome do(a) procurador(a)/assessor(a) jurídico(a) da CONTRATANTE)