PREGÃO ELETRÔNICO Nº 20210007– ETICE/DITEC
PROCESSO Nº 04358544/2021
UASG: 943001 – NÚMERO COMPRASNET: 00632022

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, para REGISTRO DE PREÇO, na forma ELETRÔNICA.

1. DO TIPO: Menor Preço.

2. DO REGIME DE EXECUÇÃO INDIRETA: Empreitada por preço unitário.

3. DA BASE LEGAL: Lei Federal nº 10.520, de 17 de julho 2002, Lei Complementar Federal 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, Decretos Estaduais nº 32.718, de 15 de junho de 2018, nº 32.824 de 11 de outubro de 2018, 33.326, de 29 de outubro de 2019, Regulamento de Licitações e Contratos da ETICE e subsidiariamente a Lei Federal nº 13.303, de 30 de junho de 2016, a Lei Federal nº 8.666, de 21 de junho de 1993 e o disposto no presente edital e seus anexos.

4. OBJETO: Registro de preços para futuras e eventuais contratações 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 no Anexo I - Termo de Referência deste edital.

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

5.1. O edital está disponível gratuitamente nos sítios www.portalcompras.ce.gov.br e https://www.gov.br/compras/pt-br/assuntos/consultas-1.

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 Robinson de Borba e Veloso.

5.3. Qualquer dúvida ou questão acerca do certame licitatório se dará exclusivamente por meio formal, mediante petição dirigida ao pregoeiro. 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 sob supervisão superior, tudo de acordo com o que dispõe a Portaria nº 091/2021, de 20 de dezembro de 2021.

5.3.1. A equipe de apoio atende pelo telefone de nº (85)3459-6370 e pelo e-mail: licitacao@pge.ce.gov.br.

6. DAS DATAS E HORÁRIOS DO CERTAME

6.1. INÍCIO DO ACOLHIMENTO DAS PROPOSTAS: 28/01/2022
6.2. DATA DE ABERTURA DAS PROPOSTAS: 09/02/2022, às 08H30
6.3. INÍCIO DA SESSÃO DE DISPUTA DE PREÇOS: 09/02/2022, às 08H30
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 realização 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: 60.811-520, CNPJ nº 06.622.070.0001-68.
7.2. Horário de expediente da Central de Licitações: das 8h às 12h e de 14h às 18h.

8. DOS RECURSOS ORÇAMENTÁRIOS

8.1.As despesas decorrentes da Ata de Registro de Preços correrão pela fonte de recursos da ETICE e dos órgão(s)/entidade(s) participante(s) do SRP (Sistema de Registro de Preços), a serem informadas quando da lavratura do instrumento de contrato.

9. DA PARTICIPAÇÃO

9.1. Os interessados em participar deste certame deverão estar credenciados junto ao portal de compras do Governo Federal.
9.1.1. As regras para credenciamento estarão disponíveis no sítio constante no subitem 5.2 deste edital.
9.2. Tratando-se de microempresas, empresas de pequeno porte e as cooperativas que se enquadrem nos termos do art. 34, da Lei Federal n° 11.488/2007, e que não se encontram em qualquer das exclusões relacionadas no § 4º do artigo 3º da Lei Complementar nº 123/2006, deverão declarar no Sistema Comprasnet para o exercício do tratamento jurídico simplificado e diferenciado previsto em Lei.
9.3. A participação implica a aceitação integral dos termos deste edital.
9.4. **É vedada a participação de licitantes nos seguintes casos:**

9.4.1. Que estejam em estado de insolvência civil, sob processo de falência, dissolução, fusão, cisão, incorporação e liquidação.
9.4.2. Cujo administrador ou sócio detentor de mais de 5% (cinco por cento) do capital social seja diretor ou empregado da ETICE.
9.4.3. Suspensas de participar de licitação com a ETICE e impedida de contratar.
9.4.4. Declaradas inidôneas pela Administração Pública, enquanto perdurarem os motivos determinantes desta condição.
9.4.5. Estrangeiras não autorizadas a comercializar no país.
9.4.6. Cujo estatuto ou contrato social, não inclua no objetivo social da empresa, atividade compatível com o objeto do certame.
9.4.7. Constituída por sócio de empresa que estiver suspensa, impedida ou declarada inidônea.
9.4.8. Cujo administrador seja sócio de empresa suspensa, impedida ou declarada inidônea.
9.4.9. Constituída por sócio que tenha sido sócio ou administrador de empresa suspensa, impedida ou declarada inidônea, no período dos fatos que deram ensejo à sanção.
9.4.10. Cujo administrador tenha sido sócio ou administrador de empresa suspensa, impedida ou declarada inidônea, no período dos fatos que deram ensejo à sanção.
9.4.11. Que tiver, nos seus quadros de diretoria, pessoa que participou, em razão de vínculo de mesma natureza, de empresa declarada inidônea.
9.4.12. Empregado ou dirigente da ETICE, como pessoa física.
9.4.13. Sob a forma de consórcio, qualquer que seja sua constituição.
9.4.13.1. As justificativas para a vedação da participação de Consórcios estão a seguir descritas.
9.4.13.1.1.A vedação de participação de Consórcios de empresas deve levar em consideração que a Jurisprudência do Tribunal de Contas da União, no Acórdão de nº 2303/2015, decidiu que a possibilidade de consórcio é um ato discricionário da Administração Pública, ou seja, é facultado à ETICE a opção de permitir ou não o consórcio nas licitações, conforme os termos do voto: “A jurisprudência consolidada desta Corte considera que a opção em permitir ou não a associação das licitantes em consórcio fica ao alvedrio do administrador”.
9.4.13.1.2. A ausência de consórcio não trará prejuízos à competitividade do certame, visto que, em regra, a formação de consórcios é admitida em casos especiais, onde empresas não costumam atender individualmente o objeto licitado em razão de sua complexidade, o que não ocorre no caso concreto, tendo em vista que, quando da obtenção das propostas, para composição do mapa de preços, não houve dificuldade; ou seja, o edital não traz em seu Termo de referência nenhuma característica própria que justificasse a admissão de empresas em consórcio.
9.4.13.1.3. Tendo em vista que é prerrogativa do Poder Público, na condição de Contratante, a escolha da participação, ou não, de empresas constituídas sob a forma de consórcio, conforme se depreende da literalidade da Lei n. 8.666/93, que em seu artigo 33 atribui à Administração a faculdade de admissão de consórcios em licitações por ela promovidas; pelos motivos já expostos, conclui-se que a vedação de constituição de empresas em consórcio, para o caso concreto, é o que melhor atende o interesse público, por prestigiar os princípios da competitividade, economicidade e moralidade.
9.4.13.1.4. Portanto, a admissão de consórcio no caso concreto atentaria contra o princípio da competitividade, pois permitiria, com o aval do Estado, a união de concorrentes que poderiam muito bem disputar entre si, violando, por via transversa, o princípio da competitividade, atingindo ainda a vantajosidade buscada pela Administração.
9.4.13.1.5. Ressalte-se que a decisão com relação à vedação à participação de consórcios visa exatamente afastar a restrição à competição, na medida que a reunião de empresas que, individualmente, poderiam prestar os serviços, reduziria o número de licitantes e poderia, eventualmente, proporcionar a formação de conluios/cartéis para manipular os preços nas licitações.
9.4.14. **Quem tenha relação de parentesco, até o terceiro grau civil, com:**
9.4.14.1**.** Dirigente ou empregado da ETICE, neste último caso quando as atribuições do empregado envolvam a atuação na área responsável pela licitação ou contratação.
9.4.14.2. Autoridade do ente público a que a ETICE esteja vinculada.
9.4.15. Cujo proprietário, mesmo na condição de sócio, tenha terminado seu prazo de gestão ou rompido seu vínculo com a ETICE. há menos de 6 (seis) meses.
9.4.16. Possuam entre seus dirigentes, gerentes, sócios, responsáveis legais ou técnicos, membros do conselho técnico, fiscal, consultivo, deliberativo ou administrativo, qualquer pessoa que seja membro da Administração da ETICE.

10. DOS PEDIDOS DE ESCLARECIMENTOS E IMPUGNAÇÕES

10.1. Os pedidos de esclarecimentos e impugnações referentes ao processo licitatório deverão ser enviados ao pregoeiro, até 3 (três) dias úteis anteriores à data fixada para abertura da sessão pública, exclusivamente por meio eletrônico, no endereço licitacao@pge.ce.gov.br, até as 17:00, no horário oficial de Brasília/DF. Indicar o nº do pregão e o pregoeiro responsável.

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

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

10.3. As respostas aos pedidos de esclarecimentos e impugnações serão divulgadas no sistema e vincularão os participantes e a administração.

10.4. Acolhida a impugnação contra este edital, será designada nova data para a realização do certame, exceto se a alteração não afetar a formulação das propostas.

11. DA HABILITAÇÃO

11.1. A licitante que for cadastrada no Sistema de Cadastramento Unificado de Fornecedores – SICAF, do Governo Federal ou Certificado de Registro Cadastral (CRC) emitido pela Secretaria do Planejamento e Gestão (SEPLAG), do Estado do Ceará, ficará dispensada da apresentação dos documentos de habilitação que constem no SICAF ou CRC.

11.1.1. A Central de Licitações verificará eletronicamente a situação cadastral, caso esteja com algum(ns) documento(s) vencido(s), a licitante deverá apresentá-lo(s) dentro do prazo de validade, sob pena de inabilitação, salvo aqueles acessíveis para consultas em *sítios* oficiais que poderão ser consultados pelo pregoeiro.

11.1.2. Existindo restrição no cadastro quanto ao documento de registro ou inscrição em entidade profissional competente, este deverá ser apresentado em situação regular, exceto quando não exigido na qualificação técnica.

11.1.3. É dever da licitante atualizar previamente os documentos constantes no SICAF ou CRC para que estejam vigentes na data da abertura da sessão pública.

11.2. Como condição prévia ao exame da documentação de habilitação da licitante detentora da proposta classificada em primeiro lugar, o pregoeiro verificará o eventual descumprimento das condições de participação, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante consulta em sites oficiais.

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

11.3. **A documentação relativa à habilitação jurídica consistirá em:**

a) Registro Comercial no caso de empresa individual.

b) Ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado, em se tratando de sociedades comerciais e, no caso de sociedades por ações, documentos de eleição de seus administradores.

c) Inscrição do ato constitutivo, no caso de sociedades civis, acompanhada de prova de diretoria em exercício.

d) Decreto de autorização, em se tratando de empresa ou sociedade estrangeira em funcionamento no país, e ato de registro ou autorização para funcionamento expedido pelo órgão competente.

e) Cédula de identidade, em se tratando de pessoa física.

11.4. **A documentação relativa à regularidade fiscal e trabalhista consistirá em:**

a) Prova de inscrição no Cadastro Nacional de Pessoa Jurídica (CNPJ).

b) Certificado de Regularidade do FGTS – CRF, perante o Fundo de Garantia por Tempo de Serviço, atualizado.

c) Prova de regularidade para com as Fazendas: Federal (Certidão Negativa de Débitos Relativos aos Tributos Federais e à Dívida Ativa da União), Estadual e Municipal do domicílio ou sede da licitante, devidamente atualizada.

d) Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante apresentação de certidão negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943, e considerando o disposto no art. 3º da Lei nº 12.440, de 07.ju.2011.

11.4.1. No caso de pessoa física, esta deverá apresentar o Cadastro de Pessoas Físicas (CPF), ficando dispensada a apresentação dos documentos “a” e “b” do item 11.4. deste edital.

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

11.4.2.1. Havendo restrição quanto à regularidade fiscal e trabalhista da microempresa, da empresa de pequeno porte ou da cooperativa que se enquadre nos termos do art. 34, da Lei Federal nº 11.488/2007, será assegurado o prazo de 5 (cinco) dias úteis, contados a partir de declarada a vencedora, para a regularização do(s) documento(s), podendo tal prazo ser prorrogado por igual período, conforme dispõe a Lei Complementar nº 123/2006.

11.4.2.2. A não comprovação da regularidade fiscal e trabalhista, até o final do prazo estabelecido, implicará na decadência do direito, sem prejuízo das sanções cabíveis, sendo facultado ao pregoeiro convocar as licitantes remanescentes, por ordem de classificação.

11.4.3. Para os estados e municípios que emitam prova de regularidade fiscal em separado, as proponentes deverão apresentar as respectivas certidões.

11.5. **A documentação relativa à qualificação técnica, consistirá em:**

11.5.1. Comprovação de aptidão para desempenho de atividades pertinentes e compatíveis em características técnicas com o objeto desta licitação, mediante apresentação de atestado(s) fornecido(s) por pessoas jurídicas de direito público ou privado, em que figurem o nome da licitante na condição de "Contratada".

11.5.2. Caso haja a apresentação de CAT (Certidão de Acervo Técnico), na qual o campo "Empresa contratada" seja em nome da licitante, a CAT substituirá a apresentação do atestado e seu respectivo contrato.

11.5.3. Esta demanda objetiva a comprovação da capacidade técnica-operacional da licitante para atender ao objeto. Para tanto, exige-se aqui, um ou mais atestados cuja a somatória de suas quantidades seja de, no mínimo, o exigido nos subitens abaixo. Estas quantidades representam um equilíbrio entre o máximo exigido para a capacidade técnica que garanta a competitividade do certame. Para tanto a licitante deve apresentar:

11.5.3.1. Atestado de capacidade técnica, fornecido por pessoa jurídica de direito público ou privado, que comprove que a licitante forneceu no mínimo 300 (trezentos) equipamentos do tipo Next Generation Firewall igual ou similar ao descrito no Termo de Referência, incluindo serviço de implantação.

11.5.3.2. Atestado de capacidade técnica, fornecido por pessoa jurídica de direito público ou privado, que comprove que a licitante forneceu suporte técnico e monitoramento em, no mínimo, 50 (cinquenta) equipamentos do tipo Next Generation Firewall.

11.5.3.3. Atestado de capacidade técnica, fornecido por pessoa jurídica de direito público ou privado, que comprove que a licitante forneceu, no mínimo, 1.400 (mil e quatrocentas) licenças de software de proteção Endpoint.

11.5.4. Todas as Declarações apresentadas deverão, explicitamente, fazer referência a este processo licitatório.

11.5.5. Os atestados deverão, obrigatoriamente, conter os dados do órgão declarante e da pessoa que assina, possibilitando sua identificação e contato.

11.5.6. A(s) declarações e o(s) atestado(s) de capacidade técnica que não esteja(m) em língua portuguesa, deverão vir acompanhados de tradução feita por tradutor juramentado.

11.5.7. DOS ATESTADOS

11..6.1. Não serão aceitos atestados emitidos pela licitante ou por empresa do mesmo grupo empresarial e/ou emitidas por empresas, das quais participem sócios ou diretores da empresa proponente.

11.6.8. A Licitante deverá entregar obrigatoriamente preenchido o Sumário de Comprovações Técnicas, conforme "ANEXO D – SUMÁRIO DE COMPROVAÇÕES TÉCNICAS" constante no "ANEXO I - Termo de Referência".

11.7. **A documentação relativa à qualificação econômica financeira, consistirá em:**

a) Certidão negativa de falência, recuperação judicial ou extrajudicial, expedida pelo distribuidor judicial da sede da pessoa jurídica.

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

11.7.1. No caso de pessoa física, esta deverá apresentar a Certidão Negativa de Execução Patrimonial expedida em domicílio, ficando dispensada a apresentação dos documentos "a" e "b" deste subitem.

11.8. A licitante deverá declarar no sistema Comprasnet, de que não emprega mão de obra que constitua violação ao disposto no inciso XXXIII, do art. 7º, da Constituição Federal.

12. DA FORMA DE APRESENTAÇÃO DA PROPOSTA ELETRÔNICA E DOCUMENTOS DE HABILITAÇÃO

12.1.As licitantes encaminharão, até a data e o horário estabelecidos para abertura da sessão pública, exclusivamente por meio do sistema, os documentos de habilitação e a proposta com a descrição do objeto ofertado e o preço, bem como declaração de responsabilidade pela autenticidade dos documentos apresentados, conforme Anexo VI – Modelo de declaração de autenticidade dos documentos deste edital.

12.1.1. Constatada a ausência da declaração de autenticidade da documentação não implicará o afastamento imediato da arrematante, por configurar falha formal passível de saneamento nos termos do subitem 23.2 deste edital.

12.1.2. A licitante deverá anexar no sistema junto à proposta de preços:

12.2. A proposta deverá explicitar nos campos "VALOR UNITÁRIO (R$)" E "VALOR TOTAL (R$)", os preços referentes a cada item, incluídos todos os custos diretos e indiretos, em conformidade com as especificações deste edital. O Campo "descrição detalhada do objeto ofertado" deverá ser preenchido.

12.2.1. No campo Valor Unitário deve ser informado:

12.2.1.1. O valor do equipamento, solução ou serviço para os itens 1 a 25;

12.2.1.2. O valor de 36 (trinta e seis) meses do serviço para os itens 26 a 30;

12.2.2. O campo Valor Total representará o resultado da multiplicação do Valor unitário pela quantidade do item.
12.2.3. A proposta deverá ser anexada, devendo a última folha ser assinada e as demais rubricadas pela licitante ou seu representante legal, redigida em língua portuguesa em linguagem clara e concisa, sem emendas, rasuras ou entrelinhas, com as especificações técnicas e quantitativos, nos termos do Anexo I-Termo de Referência deste edital.
12.2.3.1. A ausência da assinatura e rubrica não são motivos de desclassificação.
12.2.2. Prazo de validade não inferior a 90 (noventa) dias, contados a partir da data da sua emissão.
12.3. As licitantes poderão retirar ou substituir as propostas por eles apresentadas, até o término do prazo para recebimento.
12.3.1. Somente serão aceitas a realização de cotações, por prestadores de serviços, que representem 100% (cem por cento) das quantidades demandadas.
12.4. Não será estabelecida, nessa etapa do certame, ordem de classificação entre as propostas apresentadas, o que somente ocorrerá após a realização dos procedimentos de negociação e julgamento da proposta.
12.5. Os documentos que compõem a proposta e a habilitação da licitante melhor classificada somente serão disponibilizados para avaliação pelo pregoeiro e para acesso público após o encerramento do envio de lances.
12.6. Os documentos de habilitação deverão ser apresentados da seguinte forma:
12.6.1. Obrigatoriamente, da mesma sede, ou seja, se da matriz, todos da matriz, se de alguma filial, todos da mesma filial, com exceção dos documentos que são válidos tanto para matriz como para todas as filiais. O contrato será celebrado com a sede que apresentou a documentação.
12.6.2. O documento obtido através de *sítios* oficiais, que esteja condicionado à aceitação via internet, terá sua autenticidade verificada pelo pregoeiro.
12.6.3. Todos os documentos emitidos em língua estrangeira deverão ser acompanhados da tradução para língua portuguesa, efetuada por tradutor juramentado, e também consularizados ou registrados no cartório de títulos e documentos.
12.6.3.1. Documentos de procedência estrangeira, emitidos em língua portuguesa, também deverão ser apresentados consularizados ou registrados em cartório de títulos e documentos.
12.6. Dentro do prazo de validade. Na hipótese de o documento não constar expressamente o prazo de 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.

13. DA ABERTURA E ACEITABILIDADE DAS PROPOSTAS ELETRÔNICAS

13.1. Abertas as propostas, o pregoeiro fará as devidas verificações, avaliando a aceitabilidade das mesmas. Caso ocorra alguma desclassificação, deverá ser fundamentada e registrada no sistema.
13.2. Os preços deverão ser expressos em reais, com até 2 (duas) casas decimais em seus valores globais.
13.3. O sistema ordenará automaticamente as propostas classificadas pelo pregoeiro e somente estas participarão da etapa de lances.

14. DA ETAPA DE LANCES

14.1. O pregoeiro dará início à etapa competitiva no horário previsto no subitem 6.3, quando, então, as licitantes poderão encaminhar lances.
14.2. Para efeito de lances, será considerado o **valor unitário do item**.
14.3. Aberta a etapa competitiva, será considerado como primeiro lance a proposta inicial. Em seguida as licitantes poderão encaminhar lances exclusivamente por meio do sistema eletrônico, sendo a licitante imediatamente informada do seu recebimento e respectivo horário de registro e valor.
14.4. As licitantes poderão ofertar lances sucessivos, desde que inferiores ao seu último lance registrado no sistema, ainda que este seja maior que o menor lance já ofertado por outra licitante.
14.4.1. Em caso de dois ou mais lances de igual valor, prevalece aquele que for recebido e registrado em primeiro lugar.
14.5. Durante a sessão pública de disputa, as licitantes serão informadas, em tempo real, do valor do menor lance registrado. O sistema não identificará o autor dos lances ao pregoeiro nem aos demais participantes.
14.6. Será adotado para o envio de lances o modo de disputa “aberto e fechado”, em que as licitantes apresentarão lances públicos e sucessivos, com lance final e fechado.
14.7. 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.
14.8. Encerrado o prazo previsto no item 14.7., o sistema abrirá oportunidade para que a licitante da oferta de valor mais baixo e os das ofertas com preços até dez por cento superiores àquela possam ofertar um lance final e fechado em até cinco minutos, o qual será sigiloso até o encerramento deste prazo.

14.8.1. Não havendo pelo menos três ofertas nas condições definidas neste edital, poderão as licitantes dos melhores lances, 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.
14.9. Após o término dos prazos estabelecidos, o sistema ordenará os lances segundo a ordem crescente de valores.
14.9.1. Não havendo lance final e fechado classificado na forma estabelecida, haverá o reinício da etapa fechada, para que as demais licitantes, até o máximo de três, na ordem de classificação, possam ofertar um lance final e fechado em até cinco minutos, o qual será sigiloso até o encerramento deste prazo.
14.10. Poderá o pregoeiro, auxiliado pela equipe de apoio, justificadamente, admitir o reinício da etapa fechada, caso nenhuma licitante classificada na etapa de lance fechado atender às exigências de habilitação.
14.11. No caso de desconexão entre o pregoeiro e o sistema no decorrer da etapa competitiva, o sistema poderá permanecer acessível à recepção dos lances, retornando o pregoeiro, quando possível, sem prejuízos dos atos realizados.
14.12. 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 vinte e quatro horas da comunicação do fato pelo Pregoeiro aos participantes, no sítio eletrônico utilizado para divulgação.
14.13. Após o encerramento dos lances, o sistema detectará a existência de situação de empate ficto. Em cumprimento ao que determina a Lei Complementar nº 123/2006, a microempresa, a empresa de pequeno porte e a cooperativa que se enquadre nos termos do art. 34, da Lei Federal nº 11.488/2007, e que ofertou lance de até 5% (cinco por cento) superior ao menor preço da arrematante que não se enquadre nessa situação de empate, será convocada automaticamente pelo sistema, na sala de disputa, para, no prazo de 5 (cinco) minutos, utilizando-se do direito de preferência, ofertar novo lance inferior ao melhor lance registrado, sob pena de preclusão.
14.13.1. Não havendo manifestação da licitante, o sistema verificará a existência de outra em situação de empate, realizando o chamado de forma automática. Não havendo outra situação de empate, o sistema emitirá mensagem.
14.14. O sistema informará a proposta de menor preço ao encerrar a fase de disputa.

15. DA LICITANTE ARREMATANTE

15.1. O pregoeiro poderá negociar exclusivamente pelo sistema, em campo próprio, a fim de obter melhor preço.
15.2. Encerrada a etapa de envio de lances da sessão pública, o pregoeiro poderá encaminhar, pelo sistema eletrônico, contraproposta a licitante que tenha apresentado o melhor preço, para que seja obtida melhor proposta, vedada a negociação em condições diferentes das previstas neste Edital.
15.3. Definido o valor final da proposta, o pregoeiro convocará a arrematante para anexar em campo próprio do sistema, no prazo de até 24 (vinte e quatro) horas, a proposta de preços com os respectivos valores readequados ao último lance ofertado.
15.3.1. A proposta deverá ser anexada em conformidade com o item 12.2 deste edital.
15.4. Encerrada a análise quanto à aceitação da proposta, o pregoeiro verificará a habilitação da licitante, observado o disposto neste Edital.
15.5. Havendo a necessidade de envio de documentos complementares, necessários à confirmação daqueles exigidos neste Edital e já apresentados, a licitante será convocada a encaminhá-los, em formato digital, via sistema, no prazo de 2 (duas) horas, sob pena de desclassificação ou inabilitação.
15.6. O descumprimento dos prazos acima estabelecidos é causa de desclassificação da licitante, sendo convocada a licitante subsequente, e assim sucessivamente, observada a ordem de classificação.
15.7. Após a apresentação da proposta não caberá desistência.

16. DOS CRITÉRIOS DE JULGAMENTO

16.1. Para julgamento das propostas será adotado o critério de **MENOR PREÇO POR GRUPO** observadas todas as condições definidas neste edital.
16.1.1. A disputa será realizada por grupo, sendo os preços registrados em Ata, pelo valor unitário do item.
16.1.2. A proposta final para o grupo não poderá conter item com valor superior ao estimado pela administração, sob pena de desclassificação, independente do valor total do grupo.
16.2. Se a proposta de menor preço não atender as especificações, ou, ainda, se a licitante desatender às exigências habilitatórias, o pregoeiro examinará a proposta subsequente, verificando sua compatibilidade e a habilitação da participante, na ordem de classificação, e assim sucessivamente, até a apuração de uma proposta que atenda a este edital.
16.3. A licitante remanescente que esteja enquadrada no percentual estabelecido no art. 44, § 2º, da Lei Complementar nº 123/2006, no dia e hora designados pelo pregoeiro, será convocada para na sala de disputa, utilizar-se do direito de preferência, ofertando no prazo de 5 (cinco) minutos, novo lance inferior ao melhor lance registrado no item.
16.4. **Serão desclassificadas as propostas:**
16.4.1. Contenham vícios insanáveis.
16.4.2. Descumpram especificações técnicas constantes do instrumento convocatório.

16.4.3. Apresentem preços manifestamente inexequíveis, sem a apresentação da demonstração da sua exequibilidade, quando exigida.
16.4.4. Se encontrem acima do orçamento estimado para a contratação após encerrada a negociação de menor preço.
16.5. A desclassificação será sempre fundamentada e registrada no sistema.

17. DOS RECURSOS ADMINISTRATIVOS

17.1. Qualquer licitante poderá manifestar, de forma motivada, a intenção de interpor recurso, em campo próprio do sistema, no prazo de até 20 minutos depois da arrematante ser aceita e habilitada, quando lhe será concedido o prazo de 3 (três) dias para apresentação das razões do recurso no sistema do Compras-net. As demais licitantes ficam desde logo convidadas a apresentar contrarrazões dentro de igual prazo, que começará a contar a partir do término do prazo da recorrente, sendo-lhes assegurada vista imediata dos elementos indispensáveis à defesa dos seus interesses.

17.1.1. Para abertura da manifestação da intenção de recurso, o pregoeiro comunicará a retomada da sessão pública com no mínimo vinte e quatro horas de antecedência, no sítio eletrônico utilizado para realização do certame.

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

17.3. A falta de manifestação, conforme o subitem 17.1 deste edital, importará na decadência do direito de recurso.

17.4. O acolhimento de recurso importará na invalidação apenas dos atos insuscetíveis de aproveitamento.

17.5 A decisão em grau de recurso será definitiva, e dela dar-se-á conhecimento as licitantes, no endereço eletrônico constante no subitem 5.2 deste edital.

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

18.1. O sistema gerará ata circunstanciada, na qual estarão registrados todos os atos do procedimento e as ocorrências relevantes,
18.2. A homologação se dará na forma do inciso IV do art. 12 do Decreto Estadual n° 33.326/2019.
18.3. Após a homologação do resultado da licitação, os preços ofertados pelas licitantes vencedoras dos itens, serão registrados na Ata de Registro de Preços, elaborada conforme o Anexo III- Minuta da Ata de Registro de Preços, deste edital.
18.3.1. As licitantes classificadas em primeiro lugar terão o prazo de 5 (cinco) dias úteis, a contar da data do recebimento da convocação, para comparecerem perante a ETICE, 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.
18.3.1.1. A Ata de Registro de Preços, quando solicitada pela licitante, poderá ser enviada por e-mail, desde que devolvida à ETICE devidamente assinada no prazo fixado neste item.
18.4. A Ata de Registro de Preços poderá ser assinada por certificação digital.
18.5. Homologada a licitação e obedecida à sequência da classificação do certame, as licitantes serão convocadas, por meio do sistema eletrônico, para no prazo de 2 (dois) dias úteis, se assim desejarem, ajustarem seus preços ao valor da proposta da licitante mais bem classificada, visando a formação de cadastro de reserva.
18.5.1. As licitantes que aderiram ao cadastro de reserva obedecerão ao disposto no subitem 18.3.1 deste edital.
18.6. É facultada à Administração após a homologação da licitação e desde que, obedecido à ordem de classificação, convocar as licitantes remanescentes para assinarem a ata de registro de preços, em igual prazo e nas mesmas condições propostas pela vencedora, quando este não atender a convocação, ou no caso da exclusão do detentor de preço registrado, nas hipóteses previstas no art. 25 do Decreto Estadual n.º 32.824/2018.
18.6.1. Ocorrido o disposto no subitem 18.6. deste edital, respeitada a ordem de classificação, o pregoeiro convocará as licitantes do cadastro de reserva para comprovar as condições de habilitação e proposta compatível com o objeto licitado. Não havendo cadastro de reserva o pregoeiro convocará as demais remanescentes desde que realizada a negociação nas mesmas condições de habilitação e proposta da licitante vencedora. Após habilitada e classificada a licitante obedecerá ao disposto no subitem 18.3.1 deste edital.
18.7. O prazo de validade da ata de registro de preços, computadas as eventuais prorrogações, não poderá ser superior a doze meses, contado a partir da data da sua publicação.
18.8. A licitante vencedora fica obrigada a apresentar no ato da assinatura do contrato ou da ata de registro de preços, o Certificado de Registro Cadastral-CRC emitido pela Secretaria de Planejamento e Gestão do Estado do Ceará.

19. DAS SANÇÕES ADMINISTRATIVAS

19.1. A licitante que praticar quaisquer das condutas previstas nos incisos I, II, III, V, VIII, IX e X do art. 37, do Decreto Estadual nº 33.326/2019, sem prejuízo das sanções legais nas esferas civil e criminal, estará sujeita às seguintes penalidades:
19.1.1. Multa de 10% (dez por cento) sobre o valor da proposta.
19.1.2. Impedimento de licitar e contratar com a Administração, sendo, então, descredenciado no cadastro de fornecedores da Secretaria do Planejamento e Gestão (SEPLAG), do Estado do Ceará, pelo prazo de até 5 (cinco) anos, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, sem prejuízo da multa prevista neste edital e das demais cominações legais.
19.2. A licitante recolherá a multa por meio de depósito bancário em nome da ETICE, se não o fizer, será cobrada em processo de execução.
19.3. A multa poderá ser aplicada com outras sanções segundo a natureza e a gravidade da falta cometida, desde que observado o princípio da proporcionalidade.
19.4. Nenhuma sanção será aplicada sem garantia da ampla defesa e contraditório, na forma da lei.

20. DA ATA DE REGISTRO DE PREÇOS

20.1. A Empresa de Tecnologia da Informação do Ceará – ETICE será o órgão gestor da Ata de Registro de Preços de que trata este edital.
20.2. A Ata de Registro de Preços que tem caráter convocatório, elaborada conforme o Anexo III-Minuta da Ata de Registro de Preços, será assinada pelo titular da Empresa de Tecnologia da Informação do Ceará-ETICE, órgão gestor do Registro de Preços ou, por delegação, por seu substituto legal, e pelos representantes de cada um dos prestadores de serviços legalmente credenciados e identificados.
20.3. Os preços registrados na Ata de Registro de Preços serão aqueles ofertados nas propostas de preços das licitantes vencedoras e das demais interessadas em praticar os mesmos valores e condições da vencedora, conforme inciso III do art. 11 do Decreto Estadual nº 32.824/2018.
20.4. A Ata de Registro de Preços uma vez lavrada e assinada, não obriga a Administração a firmar as contratações que dela poderão advir, ficando-lhe facultada a utilização de procedimento de licitação, respeitados os dispositivos da Lei Federal 13.303/2016, sendo assegurado ao detentor do registro de preços a preferência em igualdade de condições.
20.5. O(s) órgão(s)/entidade(s) participante(s) do SRP (Sistema de Registro de Preços), quando necessitar, solicitará os serviços junto aos prestadores de serviços detentores de preços registrados na Ata de Registro de Preços, de acordo com os quantitativos e especificações previstos, durante a vigência do documento supracitado.
20.6. Os prestadores de serviços detentores de preços registrados ficarão obrigados a fornecer o objeto licitado ao(s) órgão(s)/entidade(s) participante(s) do SRP (Sistema de Registro de Preços), nos prazos, locais, quantidades e demais condições definidas no Anexo I – Termo de Referência deste edital.
20.7. A Ata de Registro de Preços, durante sua vigência, poderá ser utilizada por qualquer órgão ou entidade da Administração Pública Estadual ou de outros entes federativos, na condição de órgão interessado, mediante consulta prévia à ETICE, órgão gestor do registro de preços, conforme disciplina os artigos 19, 20, 21 e 22 do Decreto Estadual nº 32.824/2018.
20.8. Os órgãos interessados quando desejarem fazer uso da Ata de Registro de Preços, deverão manifestar seu interesse junto à ETICE, órgão gestor do Registro de Preços, a qual indicará o prestador de serviços e o preço a ser praticado.
20.8.1. As contratações decorrentes da utilização da Ata de Registro de Preços de que trata este subitem não poderão exceder, por órgão interessado, a cinquenta por cento dos quantitativos dos itens do instrumento convocatório e registrados na Ata de registro de preços.
20.8.2. O quantitativo decorrente das adesões à Ata de Registro de Preços não poderá exceder, na totalidade, ao dobro do quantitativo de cada item registrado na Ata de Registro de Preços, independentemente do número de órgãos interessados que aderirem.
20.8.3. O órgão interessado deverá efetivar a contratação solicitada em até noventa dias, contados a partir da autorização da ETICE, observado o prazo de vigência da ata.
20.8.4. A comunicação à ETICE, órgão gestor do registro de preços, acerca do cumprimento do prazo previsto no item 20.8.3. será providenciada pelo órgão interessado até o quinto dia útil após a contratação.
20.8.5. A ETICE, órgão gestor do registro de preços, não autorizará a adesão à ata de registro de preços para a contratação separada de itens de objeto adjudicado por preço global para os quais o prestador do serviço não tenha apresentado o menor preço.
20.9. Caberá à ETICE, órgão gestor do Registro de Preços, para utilização da Ata por órgãos interessados, proceder a indicação do prestador do serviço detentor do preço registrado, obedecida à ordem de classificação.
20.10. O detentor de preços registrados que descumprir as condições da Ata de Registro de Preços nos termos previstos nos incisos I a VIII do artigo 25 do Decreto Estadual n° 32.824/2018 terá o seu registro cancelado.

20.11. 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, obedecendo aos parâmetros constantes no art. 23, do Decreto Estadual n.º 32.824/2018.
20.12. A Empresa de Tecnologia da Informação do Ceará- ETICE, convocará o prestador de serviço para negociar o preço registrado e adequá-lo ao preço de mercado, sempre que verificar que o preço registrado está acima do preço de mercado. Caso seja frustrada a negociação, o fornecedor será liberado do compromisso assumido.
20.13. Não havendo êxito nas negociações com os prestadores de serviços com preços registrados, a ETICE, órgão gestor da Ata, poderá convocar os demais prestadores de serviços classificados, podendo negociar os preços de mercado, ou cancelar o item, ou ainda revogar a Ata de Registro de Preços.
20.14. Serão considerados preços de mercado, os preços que forem iguais ou inferiores à média daqueles apurados pela Administração para os itens registrados.
20.15. As alterações registradas, oriundas de revisão dos preços, serão publicadas no Diário Oficial do Estado e na página oficial do Portal Compras da Secretária de Planejamento e Gestão do Governo do Estado na internet.
20.16. As demais condições contratuais se encontram estabelecidas no Anexo IV - Minuta do Contrato.
20.17. 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(s) órgão(s)/entidade(s) participantes, o direito de adquirir o quantitativo que julgar necessário ou mesmo abster-se de adquirir o item especificado.

20.18. DA GARANTIA CONTRATUAL

20.18.1. Será exigida garantia contratual nos termos estabelecidos na cláusula nona da minuta do contrato.

20.19. DA SUBCONTRATAÇÃO

20.19.1. Será admitida a subcontratação nos termos estabelecidos na cláusula décima sexta da minuta do contrato.

21. DA FRAUDE E DA CORRUPÇÃO

21.1. As licitantes devem observar e a contratada deve observar e fazer observar, por seus fornecedores e subcontratados, se admitida subcontratação, o mais alto padrão de ética durante todo o processo de licitação, de contratação e de execução do objeto contratual. Para os propósitos deste item, definem-se as seguintes práticas:
a) “prática corrupta”: oferecer, dar, receber ou solicitar, direta ou indiretamente, qualquer vantagem com o objetivo de influenciar a ação de servidor público no processo de licitação ou na execução de contrato;
b) “prática fraudulenta”: a falsificação ou omissão dos fatos, com o objetivo de influenciar o processo de licitação ou de execução de contrato;
c) “prática conluiada”: esquematizar ou estabelecer um acordo entre duas ou mais licitantes, com ou sem o conhecimento de representantes ou prepostos do órgão licitador, visando estabelecer preços em níveis artificiais e não-competitivos;
d) “prática coercitiva”: causar dano ou ameaçar causar dano, direta ou indiretamente, às pessoas ou sua propriedade, visando a influenciar sua participação em um processo licitatório ou afetar a execução do contrato.
e) “prática obstrutiva”:
(1) destruir, falsificar, alterar ou ocultar provas em inspeções ou fazer declarações falsas aos representantes do organismo financeiro multilateral, com o objetivo de impedir materialmente a apuração de alegações de prática prevista neste subitem;
(2) atos cuja intenção seja impedir materialmente o exercício do direito de o organismo financeiro multilateral promover inspeção.
21.2. Na hipótese de financiamento, parcial ou integral, por organismo financeiro multilateral, mediante adiantamento ou reembolso, este organismo imporá sanção sobre uma empresa ou pessoa física, para a outorga de contratos financiados pelo organismo se, em qualquer momento, constatar o envolvimento da empresa, diretamente ou por meio de um agente, em práticas corruptas, fraudulentas, conluiadas, coercitivas ou obstrutivas ao participar da licitação ou da execução um contrato financiado pelo organismo.
21.3. Considerando os propósitos dos itens acima, a licitante vencedora como condição para a contratação, deverá concordar e autorizar que, na hipótese de o contrato vir a ser financiado, em parte ou integralmente, por organismo financeiro multilateral, mediante adiantamento ou reembolso, permitirá que o organismo financeiro e/ou pessoas por ele formalmente indicadas possam inspecionar o local de execução do contrato e todos os documentos e registros relacionados à licitação e à execução do contrato.
21.4. A contratante, garantida a prévia defesa, aplicará as sanções administrativas pertinentes, previstas na Lei, se comprovar o envolvimento de representante da empresa ou da pessoa física contratada em práticas corruptas, fraudulentas, conluiadas ou coercitivas, no decorrer da licitação ou na execução do contrato financiado por organismo financeiro multilateral, sem prejuízo das demais medidas administrativas, criminais e cíveis.

22. DAS DISPOSIÇÕES GERAIS

22.1. Esta licitação não importa necessariamente em contratação, podendo a autoridade competente revogá-la por razões de interesse público, anulá-la por ilegalidade de ofício ou por provocação de terceiros, mediante decisão devidamente fundamentada, sem quaisquer reclamações ou direitos à indenização ou reembolso.
22.2. 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, vedada a inclusão posterior de documentos que deveriam constar originariamente na proposta e na documentação de habilitação.
22.3. O descumprimento de prazos estabelecidos neste edital e/ou pelo pregoeiro ou o não atendimento às solicitações ensejará DESCLASSIFICAÇÃO ou INABILITAÇÃO.
22.4. Toda a documentação fará parte dos autos e não será devolvida a licitante, ainda que se trate de originais.
22.5. 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 da contratante.
22.6. Os representantes legais das licitantes são responsáveis pela fidelidade e legitimidade das informações e dos documentos apresentados em qualquer fase da licitação.
22.7. O desatendimento de exigências formais não essenciais não implicará no afastamento da licitante, desde que seja possível a aferição da sua qualificação e a exata compreensão da sua proposta.
22.8. Caberá a licitante acompanhar as operações no sistema eletrônico, ficando responsável pelo ônus decorrente da perda de negócios diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão.
22.9. O pregoeiro poderá sanar erros formais que não acarretem prejuízos para o objeto da licitação, a Administração e as licitantes, dentre estes, os decorrentes de operações aritméticas.
22.10. Os casos omissos serão resolvidos pelo pregoeiro, nos termos da legislação pertinente.
22.11. As normas que disciplinam este pregão serão sempre interpretadas em favor da ampliação da disputa.
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.

23. DOS ANEXOS

23.1. Constituem anexos deste edital, dele fazendo parte:

ANEXO I - TERMO DE REFERÊNCIA
ANEXO II - CARTA PROPOSTA
ANEXO III - MINUTA DA ATA DE REGISTRO DE PREÇOS
ANEXO IV - MINUTA DO CONTRATO
ANEXO V - MINUTA DO CONTRATO - ESTATAIS
ANEXO VI - MODELO DE DECLARAÇÃO DE AUTENTICIDADE DOS DOCUMENTOS (Anexar com a documentação de habilitação)

Fortaleza – CE, 18 de janeiro de 2022.

CIENTE:

José Lassance de Castro Silva
ORDENADOR DE DESPESA

Robinson de Borba e Veloso
PREGOEIRO

Aprovação Procuradoria Jurídica:

ANEXO I - TERMO DE REFERÊNCIA

1. UNIDADE REQUISITANTE: ETICE / DITEC

2. DO OBJETO:

2.1. Registro de preços para futuras e eventuais contratações 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.
2.2. Este objeto será realizado através de licitação na modalidade PREGÃO, na forma ELETRÔNICA, do tipo MENOR PREÇO, com a forma de fornecimento por demanda.

3. DA JUSTIFICATIVA:

3.1. As justificativas das necessidades das possíveis contratações dos itens que terão preços registrados por este Pregão Eletrônico serão fornecidas pelos órgãos participantes através de Documentos de Especificação Técnica (DET) a serem enviados a SEPLAG e atenderão a diversos projetos governamentais interligados ao Cinturão Digital do Ceará, durante a vigência da Ata de Registro de Preços, de acordo com o Artigo 3º da Instrução Normativa SEPLAG Nº 01/2017, de 13/02/2017, DO de 15/02/2017, que dispõe sobre Procedimentos para Aquisição de Bens e Serviços de TIC na Administração Pública Estadual.

3.2. JUSTIFICATIVA PARA AGRUPAMENTO DOS ITENS EM GRUPO ÚNICO:
3.2.1. Tendo em vista as características que norteiam o objeto em pauta, os itens que o compõem requerem minuciosa análise técnica quanto a sua interdependência, pois compete a Administração buscar o menor dispêndio possível de recursos, assegurando a qualidade da aquisição e/ou da prestação do serviço, o que exige a escolha da solução mais adequada e eficiente dentre as diversas opções existentes já por ocasião da definição do objeto e das condições da contratação, posto que é essa descrição que impulsiona a seleção da proposta mais vantajosa, objetivo precípuo da licitação.
3.2.2. Por se tratar de uma solução integrada, a licitação por GRUPO é mais satisfatória do ponto de vista da eficiência técnica, por consolidar as entregas a partir de um único fornecedor vencedor, gerando assim maior eficiência na gestão contratual e garantia, bem como no processo de entrega, haja vista que é notório o fato de que ao se utilizar de muitos fornecedores para entrega, aumenta-se a incidência de possibilidades de atrasos, resultando em necessidade de armazenamento de itens no almoxarifado visando a consolidação de todos os itens relacionados ao GRUPO para a localidade aplicada, consequentemente ampliando-se o custo operacional do projeto para a Administração.
3.2.3. É importante ressaltar que ao garantir entregas de soluções de um mesmo fabricante, através da licitação por GRUPO, unifica-se toda a necessidade de conhecimento técnico e operacionalização. Do contrário, abre-se a possibilidade de aquisição de soluções de fabricantes diferentes, causando impacto negativo em duas vertentes:
3.2.3.1. Recursos humanos: maior necessidade de horas/homem para fazer a gestão das soluções contratadas, uma vez que haverá necessidade de equipes distintas qualificadas em cada uma das soluções. Quando contrata-se soluções de um mesmo fabricante, uma única equipe é necessária para gerir toda a solução, diminuindo o número de horas/homem e recursos humanos para fazer a gestão de todo o ambiente. Sendo assim, perde-se economicidade, visto que a contratação de mais pessoas certamente seria necessária para a devida execução de todos os serviços em um cenário com dois fabricantes distintos.
3.2.3.2. Técnica: soluções de um mesmo fabricante permitem uma integração entre diferentes produtos, consolidando e correlacionando uma grande quantidade de informações em formato mais simplificado, diminuindo, assim, a complexidade de gestão, análise e verificação de informações e tornando, portanto, o ambiente mais seguro e com tempo de resposta significativamente menor à possíveis ataques. Ao trabalhar com soluções de fabricantes distintos essa convergência é impossibilitada, aumentando a superfície de análise das informações, tornando mais lenta a conclusão e a tomada de decisão em relação à incidentes e ameaças de segurança, exigindo também esforço elevado de um número maior de pessoas envolvidas nas soluções distintas.

3.2.4. Sendo realizado um pregão com Grupos distintos existe, ainda, a possibilidade de fracasso em um dos grupos, o que provocaria impactos administrativos, técnicos e operacionais, tendo em vista a "interdependência" entre os itens;
3.2.5. O desmembramento dos itens do objeto do pregão em mais de um Grupo, pode incorrer em dificuldades no acionamento do suporte e da garantia para resolução de problemas quando ocorrerem disfunções operacionais, já que teríamos, possivelmente, fornecedores distintos para cada um dos Grupos. Dessa maneira, entendemos que o processo de aquisição em Grupo único com todos os componentes necessários, seja ideal para a gestão e resolução de problemas por meio de um único contrato.
3.2.6. Este requisito objetiva garantir a eficiência técnica, por manter a qualidade do empreendimento, haja vista que o gerenciamento permanece todo o tempo a cargo de um mesmo administrador. Nesse ponto, busca-se a qualidade do serviço/ aquisição de forma íntegra e coordenada da solução de segurança, mantendo ainda as compatibilidades entre equipamentos e os serviços já utilizados pelo Governo do Estado, garantindo sua disponibilidade e asseverando que não haverá indefinições quanto a responsabilidade de eventuais falhas na execução contratual.
3.2.7. Além do mais, vale constar que a pesquisa de mercado se mostrou eficaz na forma como está disposto a presente contratação, ou seja, por GRUPO, não tendo sido identificado dificuldades no recebimento dos orçamentos na fase supramencionada e, por consequência, compreende-se que ao mesmo tempo em que garantimos a ampla participação do presente certame, preservaremos também o grande ganho para a Administração Pública de acordo com a economia de escala que poderá ser aplicada na execução do objeto requerido.

4. DAS ESPECIFICAÇÕES E QUANTITATIVOS

GRUPO ÚNICO – FIREWALL E SERVIÇOS CORRELATOS			
ITEM	**DESCRIÇÃO**	**Unidade de Medida**	**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	SOLUÇÃO DE NEXT GENERATION FIREWALL PARA AMBIENTES VIRTUALIZADOS EM NUVEM PRIVADA (1 QUANTIDADE PARA CADA CORE)	Unidade	30
12	SOLUÇÃO DE NEXT GENERATION FIREWALL PARA NUVEM PÚBLICA (1 QUANTIDADE PARA CADA CORE) COMPRASNET: UNIDADE = SERVIÇO	Serviço	30
13	SOLUÇÃO DE SEGURANÇA E VISIBILIDADE PARA AMBIENTES MULTI-CLOUD COMPRASNET: UNIDADE = SERVIÇO	Serviço	4
14	SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO E RELATÓRIOS PARA ATÉ 5 EQUIPAMENTOS COMPRASNET: UNIDADE = SERVIÇO	Serviço	8
15	SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO E RELATÓRIOS PARA ATÉ 10 EQUIPAMENTOS COMPRASNET: UNIDADE = SERVIÇO	Serviço	6
16	SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO E RELATÓRIOS PARA ATÉ 50 EQUIPAMENTOS COMPRASNET: UNIDADE = SERVIÇO	Serviço	4
17	SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO E RELATÓRIOS PARA ILIMITADOS EQUIPAMENTOS COMPRASNET: UNIDADE = SERVIÇO	Serviço	4

18	SOLUÇÃO DE NEXT GENERATION ANTI-MALWARE PARA NOTEBOOKS, DESKTOPS E SERVIDORES COMPRASNET: UNIDADE = SERVIÇO	Serviço	10000
19	SOLUÇÃO DE PREVENÇÃO DE AMEAÇAS PARA DISPOSITIVOS MÓVEIS ANDROID E IOS COMPRASNET: UNIDADE = SERVIÇO	Serviço	5000
20	SOLUÇÃO DE ACESSO REMOTO SEGURO (SASE) COMPRASNET: UNIDADE = SERVIÇO	Serviço	5000
21	INSTALAÇÃO FIREWALL UNIDADE ATÉ 100KM COMPRASNET: UST = SERVIÇO	Serviço	500
22	INSTALAÇÃO FIREWALL UNIDADE ATÉ 400KM COMPRASNET: UST = SERVIÇO	Serviço	300
23	INSTALAÇÃO FIREWALL UNIDADE ACIMA DE 400KM COMPRASNET: UST = SERVIÇO	Serviço	300
24	INSTALAÇÃO FIREWALL SEDE COMPRASNET: UST = SERVIÇO	Serviço	36
25	INSTALAÇÃO FIREWALL DATA CENTER COMPRASNET: UST = SERVIÇO	Serviço	16
26	SERVIÇO DE MONITORAMENTO E SUPORTE TECNICO 24X7 DE FIREWALL UNIDADE TIPO 1 E 2 - 36 MESES COMPRASNET: UST = SERVIÇO	Serviço	1050
27	SERVIÇO DE MONITORAMENTO E SUPORTE TECNICO 24X7 DE FIREWALL UNIDADE TIPO 3 E 4 - 36 MESES COMPRASNET: UST = SERVIÇO	Serviço	30
28	SERVIÇO DE MONITORAMENTO E SUPORTE TÉCNICO 24X7 DE FIREWALL SEDE – 36 MESES COMPRASNET: UST = SERVIÇO	Serviço	28
29	SERVIÇO DE MONITORAMENTO E SUPORTE TÉCNICO 24X7 DE FIREWALL DATA CENTER – 36 MESES COMPRASNET: UST = SERVIÇO	Serviço	14
30	SERVIÇO DE SOC 24X7 COM SIEM – PACOTES DE 200 EPS – 36 MESES COMPRASNET: UNIDADE = SERVIÇO	Serviço	30

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

4.1. ESPECIFICAÇÃO DETALHADA:

4.1.1. ITEM 1 – NEXT GENERATION FIREWALL – UNIDADE TIPO I

4.1.2. CARACTERÍSTICAS GERAIS

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

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

4.1.2.3. 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;

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

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

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

4.1.2.7. 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.

4.1.3. CAPACIDADE E QUANTIDADES

4.1.3.1. 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;

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

4.1.3.3. Suporte a, no mínimo, 10.300 (dez mil e trezentas) novas conexões ou sessões por segundo;
4.1.3.4. Throughput de, no mínimo, 950 Mbps para conexões VPN;
4.1.3.5. Licenciado ou permitir, pelo menos, 100 conexões ou sessões simultâneas de VPN client-to-site;
4.1.3.6. Possuir, pelo menos, 6 (seis) interfaces de rede 1Gbps UTP;
4.1.3.7. Possuir 1 (uma) interface do tipo console ou similar;
4.1.3.8. 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;
4.1.4. FUNCIONALIDADES DE FIREWALL
4.1.4.1. Deve suportar autenticação para o serviço NTP.
4.1.4.2. Deve ser possível definir por quais origens de rede são permitidas as conexões do administrador. 4.1.4.3. Deve ser possível restringir o acesso à gerência do equipamento por, pelo menos, endereço IP e Rede.
4.1.4.4. Deve suportar SNMP v2 e v3.
4.1.4.5. Deve ser possível realizar captura de pacotes diretamente na gerência do equipamento.
4.1.4.6. Deve ser possível monitorar a utilização de CPU e memória diretamente na gerência do equipamento.
4.1.4.7. Deve ser possível realizar a configuração do cluster diretamente na gerência do equipamento.
4.1.4.8. Deve ser possível conectar a serviços de DDNS;
4.1.4.9. Deve ser possível configurar o timeout da sessão do administrador na interface web.
4.1.4.10. Deve ser possível configurar a complexidade da senha do administrador e dias para expirar.
4.1.4.11. A solução deve ser capaz de trabalhar com identidades de usuários para propósitos de configurações e logs.
4.1.4.12. 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;
4.1.4.13. A solução deve identificar usuários das seguintes fontes pelo menos:
4.1.4.14. Active Directory: o gateway de segurança deve realizar consulta aos servidores AD para obter informação dos usuários;
4.1.4.15. Autenticação via navegador: para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador;
4.1.4.16. 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;
4.1.4.17. 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;

4.1.5. Funcionalidade de Prevenção de Ameaças
4.1.5.1. 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.
4.1.5.2. 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;
4.1.5.3. Deve ser possível realizar a atualização manualmente sem necessidade de internet através da importação do pacote de atualização.
4.1.5.4. 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;
4.1.5.5. Deve ser capaz de bloquear tráfego SSH em DNS tunneling;
4.1.5.6. A solução deverá ser capaz de inspecionar e proteger apenas hosts internos ou inspecionar todo o tráfego;
4.1.5.7. A solução deve proteger contra ataques do tipo envenenamento de cache DNS (DNS Cache Poisoning);

4.1.5.8. A solução deverá possuir pelo menos dois perfis pré-configurados de fábrica para uso imediato e permitir a customização de um perfil;
4.1.5.9. 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;
4.1.5.10. 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;
4.1.5.11. 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.
4.1.5.12. Deve ser possível visualizar a lista de proteções disponíveis no equipamento com os detalhes.
4.1.5.13. 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).
4.1.5.14. A solução deve bloquear arquivos potencialmente maliciosos infectados com malware.
4.1.5.15. A solução de proteção contra malware e bot deve compartilhar a mesma política para facilitar o gerenciamento.
4.1.5.16. 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;
4.1.5.17. As proteções devem ser ativadas baseadas em, pelo menos, critério de nível de confiança, ações da proteção e impacto de performance.
4.1.5.18. Deve ser possível habilitar a trilha das proteções para não logar, criar um log ou gerar um alerta;
4.1.5.19. 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.
4.1.5.20. A solução de anti-malware deve suportar protocolos SMTP e POP3, FTP, HTTP em qualquer porta;
4.1.5.21. Deve ser possível definir uma política de inspeção para os tipos de arquivos por:
4.1.5.21.1. Inspecionar tipos de arquivos conhecidos que contenham malware;
4.1.5.21.2. Inspecionar todos os tipos de arquivos;
4.1.5.21.3. Inspecionar tipos de arquivos de famílias específicas;
4.1.5.21.4. Deve bloquear acesso a URLs com malware;
4.1.5.22. Deve ser possível customizar a página exibida para o usuário quando a URL contiver um malware e o acesso for bloqueado;

4.1.6. FILTRO DE CONTEÚDO WEB
4.1.6.1. 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;
4.1.6.2. A gerência das políticas de segurança de controle de aplicação e controle de URL's deverá ser realizada na mesma interface web de gerenciamento;
4.1.6.3. 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.
4.1.6.4. Deve ser possível configurar com apenas um clique o bloqueio a sites com conteúdo inapropriado como sexo, violência, armas, jogos e álcool.
4.1.6.5. Deve configurar regras para permitir ou bloquear aplicações ou páginas da Internet por pelo menos:
4.1.6.5.1. Usuário do Active Directory
4.1.6.5.2. IP
4.1.6.5.3. Rede
4.1.6.6. Deve ser possível configurar o bloqueio de compartilhamento de arquivos com origem usualmente ilegais como aplicações torrents e peer-to-peer.
4.1.6.7. Deve ser possível configurar manualmente o bloqueio de aplicações ou categorias de sites de aplicações indesejadas.
4.1.6.8. Deve ainda ser possível adicionar uma URL ou aplicação que não está na base de dados.
4.1.6.9. Deve ser possível limitar o consumo de banda de aplicações.

4.1.6.10. 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;
4.1.6.11. Deve ser possível realizar a recategorização de uma URL através da gerência do equipamento.
4.1.6.12. Deve ser possível customizar e definir a frequência com que serão exibidas as mensagens para os usuários nas seguintes ações:
4.1.6.12.1. Aceitar e informar
4.1.6.12.2. Bloquear e informar
4.1.6.12.3. Perguntar
4.1.7. IDENTIFICAÇÃO DE USUÁRIOS
4.1.7.1. A solução deve ser capaz de trabalhar com identidades de usuários para propósitos de configurações e logging.
4.1.7.2. A solução deve possibilitar ao administrador realizar a integração com o AD através de um assistente de configuração na própria interface gráfica do produto;
4.1.7.3. A solução deve identificar usuários das seguintes fontes:
4.1.7.3.1. Active Directory - o gateway de segurança deve realizar consulta aos servidores AD para obter informação dos usuários;
4.1.7.3.2. Autenticação via navegador - Para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador;
4.1.7.4. 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;
4.1.7.5. 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;
4.1.8. FUNCIONALIDADES DE ACESSO REMOTO
4.1.8.1. A solução deve prover acesso seguro encriptado aos usuários remotos através da Internet;
4.1.8.2. A solução deve prover conectividade através de um cliente instalado no computador do usuário e através do navegador do usuário com conexão segura (HTTPS).
4.1.8.3. Deve suportar pelo menos os seguintes métodos de conexão:
4.1.8.3.1. Conexão através de cliente instalado no laptop ou desktop do usuário.
4.1.8.3.2. Conexão através de cliente instalado no smartphone e tablets.
4.1.8.3.3. Conexão através de navegador com SSL.
4.1.8.3.4. Conexão através de cliente nativo Windows L2TP.
4.1.8.4. Solução deve suportar alterar a porta padrão 443 para estabelecimento de VPN SSL.
4.1.8.5. A solução deve permitir conexão VPN aos seguintes usuários:
4.1.8.5.1. Usuários locais na própria base do appliance.
4.1.8.5.2. Grupos de usuários locais na própria base do appliance.
4.1.8.5.3. Grupos de usuários do Active Directory.
4.1.8.5.4. Grupos de usuários Radius.
4.1.8.6. A solução deve permitir atribuir um endereço específico para o usuário remoto.

4.1.9. FUNCIONALIDADE DE VPN SITE-TO-SITE
4.1.9.1. A solução deve prover acesso seguro criptografado entre duas localidades através da Internet;
4.1.9.2. A solução deve estabelecer VPN com o site remoto do próprio fabricante ou de terceiros;
4.1.9.3. A solução deve suportar autenticação com senha ou certificado;
4.1.9.4. Deve suportar, pelo menos, criptografia AES 128 e 256;
4.1.9.5. Deve possuir mecanismo para monitorar a saúde do túnel remoto;
4.1.9.6. Quando o túnel for estabelecido entre dispositivos do mesmo fabricante este deve possuir protocolo proprietário para testar se o túnel está ativo.
4.2. ITEM 2 – NEXT GENERATION FIREWALL – UNIDADE TIPO II
4.2.1. CARACTERÍSTICAS GERAIS
4.2.1.1. É permitida a composição da solução ofertada entre diversos fabricantes, desde que não contemple solução de software livre;
4.2.1.2. A solução deverá ser compatível com SNMPv2 e SNMPv3;
4.2.1.3. 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;

4.2.1.4. A comunicação entre os appliances de segurança e o módulo de gerência deve ser através de meio criptografado;
4.2.1.5. Os appliances de segurança devem suportar operar em cluster ativo-ativo e ativo-passivo sem a necessidade de licenças adicionais;
4.2.1.6. Não serão aceitos modelos em listas de end-of-sale, cuja data do fim de vendas seja anterior à data da proposta.
4.2.1.7. 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.

4.2.2. CAPACIDADE E QUANTIDADES
4.2.2.1. 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;
4.2.2.2. Suporte a, no mínimo, 490.000 (quatrocentas e noventa mil) conexões ou sessões simultâneas;
4.2.2.3. Suporte a, no mínimo, 20.000 (vinte mil) novas conexões ou sessões por segundo;
4.2.2.4. Throughput de, no mínimo, 2.2 Gbps para conexões VPN;
4.2.2.5. Licenciado ou permitir, pelo menos, 200 conexões ou sessões simultâneas de VPN client-to-site;
4.2.2.6. Possuir, pelo menos, 10 (dez) interfaces de rede 1Gbps UTP;
4.2.2.7. Possuir, pelo menos, 1 (uma) interface de rede 1Gbps SFP;
4.2.2.8. Possuir 1 (uma) interface do tipo console ou similar;
4.2.2.9. 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;

4.2.3. FUNCIONALIDADES DE FIREWALL
4.2.3.1. Deve suportar autenticação para o serviço NTP.
4.2.3.2. Deve ser possível definir por quais origens de rede são permitidas as conexões do administrador.
4.2.3.3. Deve ser possível restringir o acesso à gerência do equipamento por, pelo menos, endereço IP e Rede.
4.2.3.4. Deve suportar SNMP v2 e v3.
4.2.3.5. Deve ser possível realizar captura de pacotes diretamente na gerência do equipamento.
4.2.3.6. Deve ser possível monitorar a utilização de CPU e memória diretamente na gerência do equipamento.
4.2.3.7. Deve ser possível realizar a configuração do cluster diretamente na gerência do equipamento.
4.2.3.8. Deve ser possível conectar a serviços de DDNS;
4.2.3.9. Deve ser possível configurar o timeout da sessão do administrador na interface web.
4.2.3.10. Deve ser possível configurar a complexidade da senha do administrador e dias para expirar.
4.2.3.11. A solução deve ser capaz de trabalhar com identidades de usuários para propósitos de configurações e logs.
4.2.3.12. 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;
4.2.3.13. A solução deve identificar usuários das seguintes fontes pelo menos:
4.2.3.14. Active Directory: o gateway de segurança deve realizar consulta aos servidores AD para obter informação dos usuários;
4.2.3.15. Autenticação via navegador: para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador;
4.2.3.16. 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;
4.2.3.17. 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;

4.2.4. FUNCIONALIDADE DE PREVENÇÃO DE AMEAÇAS

4.2.4.1. 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.

4.2.4.2. 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;

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

4.2.4.4. 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;

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

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

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

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

4.2.4.9. 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;

4.2.4.10. 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;

4.2.4.11. 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.

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

4.2.4.13. 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).

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

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

4.2.4.16. 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;

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

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

4.2.4.19. 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.

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

4.2.4.21. Deve ser possível definir uma política de inspeção para os tipos de arquivos por:

4.2.4.21.1. Inspecionar tipos de arquivos conhecidos que contenham malware;

4.2.4.21.2. Inspecionar todos os tipos de arquivos;

4.2.4.21.3. Inspecionar tipos de arquivos de famílias específicas;

4.2.4.22. Deve bloquear acesso a URLs com malware;

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

4.2.5. FILTRO DE CONTEÚDO WEB

4.2.5.1. 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;

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

4.2.5.3. 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.
4.2.5.4. Deve ser possível configurar com apenas um clique o bloqueio a sites com conteúdo inapropriado como sexo, violência, armas, jogos e álcool.
4.2.5.5. Deve configurar regras para permitir ou bloquear aplicações ou páginas da Internet por pelo menos:
4.2.5.5.1. Usuário do Active Directory
4.2.5.5.2. IP
4.2.5.5.3. Rede
4.2.5.6. Deve ser possível configurar o bloqueio de compartilhamento de arquivos com origem usualmente ilegais como aplicações torrents e peer-to-peer.
4.2.5.7. Deve ser possível configurar manualmente o bloqueio de aplicações ou categorias de sites de aplicações indesejadas.
4.2.5.8. Deve ainda ser possível adicionar uma URL ou aplicação que não está na base de dados.
4.2.5.9. Deve ser possível limitar o consumo de banda de aplicações.
4.2.5.10. 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;
4.2.5.11. Deve ser possível realizar a recategorização de uma URL através da gerência do equipamento.
4.2.5.12. Deve ser possível customizar e definir a frequência com que serão exibidas as mensagens para os usuários nas seguintes ações:
4.2.5.12.1. Aceitar e informar
4.2.5.12.2. Bloquear e informar
4.2.5.12.3. Perguntar

4.2.6. IDENTIFICAÇÃO DE USUÁRIOS
4.2.6.1. A solução deve ser capaz de trabalhar com identidades de usuários para propósitos de configurações e logging.
4.2.6.2. A solução deve possibilitar ao administrador realizar a integração com o AD através de um assistente de configuração na própria interface gráfica do produto;
4.2.6.3. A solução deve identificar usuários das seguintes fontes:
4.2.6.3.1. Active Directory - o gateway de segurança deve realizar consulta aos servidores AD para obter informação dos usuários;
4.2.6.3.2. Autenticação via navegador - Para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador;
4.2.6.4. 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;
4.2.6.5. 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;

4.2.7. FUNCIONALIDADES DE ACESSO REMOTO
4.2.7.1. A solução deve prover acesso seguro encriptado aos usuários remotos através da Internet;
4.2.7.2. A solução deve prover conectividade através de um cliente instalado no computador do usuário e através do navegador do usuário com conexão segura (HTTPS).
4.2.7.3. Deve suportar pelo menos os seguintes métodos de conexão:
4.2.7.3.1. Conexão através de cliente instalado no laptop ou desktop do usuário.
4.2.7.3.2. Conexão através de cliente instalado no smartphone e tablets.
4.2.7.3.3. Conexão através de navegador com SSL.
4.2.7.3.4. Conexão através de cliente nativo Windows L2TP.
4.2.7.4. Solução deve suportar alterar a porta padrão 443 para estabelecimento de VPN SSL.
4.2.7.5. A solução deve permitir conexão VPN aos seguintes usuários:
4.2.7.5.1. Usuários locais na própria base do appliance.
4.2.7.5.2. Grupos de usuários locais na própria base do appliance.
4.2.7.5.3. Grupos de usuários do Active Directory.
4.2.7.5.4. Grupos de usuários Radius.

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

4.2.8. FUNCIONALIDADE DE VPN SITE-TO-SITE
4.2.8.1. A solução deve prover acesso seguro criptografado entre duas localidades através da Internet;
4.2.8.2. A solução deve estabelecer VPN com o site remoto do próprio fabricante ou de terceiros;
4.2.8.3. A solução deve suportar autenticação com senha ou certificado;
4.2.8.4. Deve suportar, pelo menos, criptografia AES 128 e 256;
4.2.8.5. Deve possuir mecanismo para monitorar a saúde do túnel remoto;
4.2.8.6. Quando o túnel for estabelecido entre dispositivos do mesmo fabricante este deve possuir protocolo proprietário para testar se o túnel está ativo

.

4.3. ITEM 3 – NEXT GENERATION FIREWALL – UNIDADE TIPO III

4.3.1. CARACTERÍSTICAS GERAIS
4.3.1.1. É permitida a composição da solução ofertada entre diversos fabricantes, desde que não contemple solução de software livre;
4.3.1.2. A solução deverá ser compatível com SNMPv2 e SNMPv3;
4.3.1.3. 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;
4.3.1.4. A comunicação entre os appliances de segurança e o módulo de gerência deve ser através de meio criptografado;
4.3.1.5. Os appliances de segurança devem suportar operar em cluster ativo-ativo e ativo-passivo sem a necessidade de licenças adicionais;
4.3.1.6. Não serão aceitos modelos em listas de end-of-sale, cuja data do fim de vendas seja anterior à data da proposta.
4.3.1.7. 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.

4.3.2. CAPACIDADE E QUANTIDADES
4.3.2.1. Throughput de, no mínimo, 1.45 Gbps, com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação, anti-malware e prevenção de ameaças avançadas (dia zero) habilitados simultaneamente;
4.3.2.2. Suporte a, no mínimo, 2.3 (dois ponto três) milhões de conexões ou sessões simultâneas;
4.3.2.3. Suporte a, no mínimo, 50.000 (cinquenta mil) novas conexões ou sessões por segundo;
4.3.2.4. Throughput de, no mínimo, 3 Gbps para conexões VPN;
4.3.2.5. Licenciado ou permitir, pelo menos, 450 conexões ou sessões simultâneas de VPN client-to-site;
4.3.2.6. Possuir, pelo menos, 16 (dezesseis) interfaces de rede 1 Gbps UTP;
4.3.2.7. Pòssuir, pelo menos, 2 (duas) interfaces de rede 1Gbps SFP;
4.3.2.8. Possuir 1 (uma) interface do tipo console ou similar;
4.3.2.9. 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;
4.3.3. FUNCIONALIDADES DE FIREWALL
4.3.3.1. Deve suportar autenticação para o serviço NTP.
4.3.3.2. Deve ser possível definir por quais origens de rede são permitidas as conexões do administrador.
4.3.3.3. Deve ser possível restringir o acesso à gerência do equipamento por, pelo menos, endereço IP e Rede.
4.3.3.4. Deve suportar SNMP v2 e v3.
4.3.3.5. Deve ser possível realizar captura de pacotes diretamente na gerência do equipamento.
4.3.3.6. Deve ser possível monitorar a utilização de CPU e memória diretamente na gerência do equipamento.
4.3.3.7. Deve ser possível realizar a configuração do cluster diretamente na gerência do equipamento.
4.3.3.8. Deve ser possível conectar a serviços de DDNS;
4.3.3.9. Deve ser possível configurar o timeout da sessão do administrador na interface web.
4.3.3.10. Deve ser possível configurar a complexidade da senha do administrador e dias para expirar.
4.3.3.11. A solução deve ser capaz de trabalhar com identidades de usuários para propósitos de configurações e logs.
4.3.3.12. 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;
4.3.3.13. A solução deve identificar usuários das seguintes fontes pelo menos:

4.3.3.14. Active Directory: o gateway de segurança deve realizar consulta aos servidores AD para obter informação dos usuários;
4.3.3.15. Autenticação via navegador: para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador;
4.3.3.16. 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;
4.3.3.17. 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;

4.3.4. FUNCIONALIDADE DE PREVENÇÃO DE AMEAÇAS
4.3.4.1. 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.
4.3.4.2. 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;
4.3.4.3. Deve ser possível realizar a atualização manualmente sem necessidade de internet através da importação do pacote de atualização.
4.3.4.4. 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;
4.3.4.5. Deve ser capaz de bloquear tráfego SSH em DNS tunneling;
4.3.4.6. A solução deverá ser capaz de inspecionar e proteger apenas hosts internos ou inspecionar todo o tráfego;
4.3.4.7. A solução deve proteger contra ataques do tipo envenenamento de cache DNS (DNS Cache Poisoning);
4.3.4.8. A solução deverá possuir pelo menos dois perfis pré-configurados de fábrica para uso imediato e permitir a customização de um perfil;
4.3.4.9. 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;
4.3.4.10. 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;
4.3.4.11. 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.
4.3.4.12. Deve ser possível visualizar a lista de proteções disponíveis no equipamento com os detalhes.
4.3.4.13. 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 & control).
4.3.4.14. A solução deve bloquear arquivos potencialmente maliciosos infectados com malware.
4.3.4.15. A solução de proteção contra malware e bot deve compartilhar a mesma política para facilitar o gerenciamento.
4.3.4.16. 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;
4.3.4.17. As proteções devem ser ativadas baseadas em, pelo menos, critério de nível de confiança, ações da proteção e impacto de performance.
4.3.4.18. Deve ser possível habilitar a trilha das proteções para não logar, criar um log ou gerar um alerta;
4.3.4.19. 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.
4.3.4.20. A solução de anti-malware deve suportar protocolos SMTP e POP3, FTP, HTTP em qualquer porta;
4.3.4.21. Deve ser possível definir uma política de inspeção para os tipos de arquivos por:
4.3.4.21.1. Inspecionar tipos de arquivos conhecidos que contenham malware;
4.3.4.21.2. Inspecionar todos os tipos de arquivos;
4.3.4.21.3. Inspecionar tipos de arquivos de famílias específicas;
4.3.4.22. Deve bloquear acesso a URLs com malware;

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

4.3.5. PREVENÇÃO DE AMEAÇAS AVANÇADAS
4.3.5.1. 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.
4.3.5.2. A solução deve compartilhar a mesma política da proteção contra vírus e bot para facilitar o gerenciamento.
4.3.5.3. A solução deve trabalhar em modo de prevenção e não apenas detecção.
4.3.5.4. Deve permitir criar uma lista de exceção de e-mails que não devem ter seus anexos inspecionados.
4.3.5.5. Deve permitir criar uma lista de exceção para arquivos que não devem ser inspecionados.
4.3.5.6. A solução deve suportar protocolos SMTP, HTTP em qualquer porta;
4.3.5.7. Deve permitir configurar por tipo de arquivo as ações de inspeção ou bypass.
4.3.5.8. 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
4.3.5.9. Implementar detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF com tamanho até 15 Mb.
4.3.5.10. 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.

4.3.6. FILTRO DE CONTEÚDO WEB
4.3.6.1. 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;
4.3.6.2. A gerência das políticas de segurança de controle de aplicação e controle de URL's deverá ser realizada na mesma interface web de gerenciamento;
4.3.6.3. 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.
4.3.6.4. Deve ser possível configurar com apenas um clique o bloqueio a sites com conteúdo inapropriado como sexo, violência, armas, jogos e álcool.
4.3.6.5. Deve configurar regras para permitir ou bloquear aplicações ou páginas da Internet por pelo menos:
4.3.6.5.1. Usuário do Active Directory
4.3.6.5.2. IP
4.3.6.5.3. Rede
4.3.6.6. Deve ser possível configurar o bloqueio de compartilhamento de arquivos com origem usualmente ilegais como aplicações torrents e peer-to-peer.
4.3.6.7. Deve ser possível configurar manualmente o bloqueio de aplicações ou categorias de sites de aplicações indesejadas.
4.3.6.8. Deve ainda ser possível adicionar uma URL ou aplicação que não está na base de dados.
4.3.6.9. Deve ser possível limitar o consumo de banda de aplicações.
4.3.6.10. 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;
4.3.6.11. Deve ser possível realizar a recategorização de uma URL através da gerência do equipamento.
4.3.6.12. Deve ser possível customizar e definir a frequência com que serão exibidas as mensagens para os usuários nas seguintes ações:
4.3.6.12.1. Aceitar e informar
4.3.6.12.2. Bloquear e informar
4.3.6.12.3. Perguntar

4.3.7. IDENTIFICAÇÃO DE USUÁRIOS

4.3.7.1. A solução deve ser capaz de trabalhar com identidades de usuários para propósitos de configurações e logging.
4.3.7.2. A solução deve possibilitar ao administrador realizar a integração com o AD através de um assistente de configuração na própria interface gráfica do produto;
4.3.7.3. A solução deve identificar usuários das seguintes fontes:
4.3.7.3.1. Active Directory - o gateway de segurança deve realizar consulta aos servidores AD para obter informação dos usuários;
4.3.7.3.2. Autenticação via navegador - Para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador;
4.3.7.4. 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;
4.3.7.5. 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;

4.3.8. FUNCIONALIDADES DE ACESSO REMOTO
4.3.8.1. A solução deve prover acesso seguro encriptado aos usuários remotos através da Internet;
4.3.8.2. A solução deve prover conectividade através de um cliente instalado no computador do usuário e através do navegador do usuário com conexão segura (HTTPS).
4.3.8.3. Deve suportar pelo menos os seguintes métodos de conexão:
4.3.8.4. Conexão através de cliente instalado no laptop ou desktop do usuário.
4.3.8.5. Conexão através de cliente instalado no smartphone e tablets.
4.3.8.6. Conexão através de navegador com SSL.
4.3.8.7. Conexão através de cliente nativo Windows L2TP.
4.3.8.8. Solução deve suportar alterar a porta padrão 443 para estabelecimento de VPN SSL.
4.3.8.9. A solução deve permitir conexão VPN aos seguintes usuários:
4.3.8.9.1. Usuários locais na própria base do appliance.
4.3.8.9.2. Grupos de usuários locais na própria base do appliance.
4.3.8.9.3. Grupos de usuários do Active Directory.
4.3.8.9.4. Grupos de usuários Radius.
4.3.8.10. A solução deve permitir atribuir um endereço específico para o usuário remoto.

4.3.9. FUNCIONALIDADE DE VPN SITE-TO-SITE
4.3.9.1. A solução deve prover acesso seguro criptografado entre duas localidades através da Internet;
4.3.9.2. A solução deve estabelecer VPN com o site remoto do próprio fabricante ou de terceiros;
4.3.9.3. A solução deve suportar autenticação com senha ou certificado;
4.3.9.4. Deve suportar, pelo menos, criptografia AES 128 e 256;
4.3.9.5. Deve possuir mecanismo para monitorar a saúde do túnel remoto;
4.3.9.6. Quando o túnel for estabelecido entre dispositivos do mesmo fabricante este deve possuir protocolo proprietário para testar se o túnel está ativo.

4.4. ITEM 4 – NEXT GENERATION FIREWALL – UNIDADE TIPO IV

4.4.1. CARACTERÍSTICAS GERAIS
4.4.1.1. É permitida a composição da solução ofertada entre diversos fabricantes, desde que não contemple solução de software livre;
4.4.1.2. A solução deverá ser compatível com SNMPv2 e SNMPv3;
4.4.1.3. 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;
4.4.1.4. A comunicação entre os appliances de segurança e o módulo de gerência deve ser através de meio criptografado;
4.4.1.5. Os appliances de segurança devem suportar operar em cluster ativo-ativo e ativo-passivo sem a necessidade de licenças adicionais;

4.4.1.6. Não serão aceitos modelos em listas de end-of-sale, cuja data do fim de vendas seja anterior à data da proposta.
4.4.1.7. 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.

4.4.2. CAPACIDADE E QUANTIDADES
4.4.2.1. 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;
4.4.2.2. Suporte a, no mínimo, 2.3 (dois ponto três) milhões de conexões ou sessões simultâneas;
4.4.2.3. Suporte a, no mínimo, 65.000 (sessenta e cinco mil) novas conexões ou sessões por segundo;
4.4.2.4. Throughput de, no mínimo, 3.8 Gbps para conexões VPN;
4.4.2.5. Licenciado ou permitir, pelo menos, 450 conexões ou sessões simultâneas de VPN client-to-site;
4.4.2.6. Possuir, pelo menos, 16 (dezesseis) interfaces de rede 1 Gbps UTP;
4.4.2.7. Possuir, pelo menos, 1 (uma) interfaces de rede 1Gbps SFP;
4.4.2.8. Possuir, pelo menos, 1 (uma) interface de rede 10Gbps SFP+;
4.4.2.9. Possuir armazenamento interno de, pelo menos, 250 GB SSD;
4.4.2.10. Possuir 1 (uma) interface do tipo console ou similar;
4.4.2.11. 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;

4.4.3. FUNCIONALIDADES DE FIREWALL
4.4.3.1. Deve suportar autenticação para o serviço NTP.
4.4.3.2. Deve ser possível definir por quais origens de rede são permitidas as conexões do administrador.
4.4.3.3. Deve ser possível restringir o acesso à gerência do equipamento por, pelo menos, endereço IP e Rede.
4.4.3.4. Deve suportar SNMP v2 e v3.
4.4.3.5. Deve ser possível realizar captura de pacotes diretamente na gerência do equipamento.
4.4.3.6. Deve ser possível monitorar a utilização de CPU e memória diretamente na gerência do equipamento.
4.4.3.7. Deve ser possível realizar a configuração do cluster diretamente na gerência do equipamento.
4.4.3.8. Deve ser possível conectar a serviços de DDNS;
4.4.3.9. Deve ser possível configurar o timeout da sessão do administrador na interface web.
4.4.3.10. Deve ser possível configurar a complexidade da senha do administrador e dias para expirar.
4.4.3.11. A solução deve ser capaz de trabalhar com identidades de usuários para propósitos de configurações e logs.
4.4.3.12. 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;
4.4.3.13. A solução deve identificar usuários das seguintes fontes pelo menos:
4.4.3.14. Active Directory: o gateway de segurança deve realizar consulta aos servidores AD para obter informação dos usuários;
4.4.3.15. Autenticação via navegador: para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador;
4.4.3.16. 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;
4.4.3.17. 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;

4.4.4. FUNCIONALIDADE DE PREVENÇÃO DE AMEAÇAS

4.4.4.1. 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.
4.4.4.2. 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;
4.4.4.3. Deve ser possível realizar a atualização manualmente sem necessidade de internet através da importação do pacote de atualização.
4.4.4.4. 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;
4.4.4.5. Deve ser capaz de bloquear tráfego SSH em DNS tunneling;
4.4.4.6. A solução deverá ser capaz de inspecionar e proteger apenas hosts internos ou inspecionar todo o tráfego;
4.4.4.7. A solução deve proteger contra ataques do tipo envenenamento de cache DNS (DNS Cache Poisoning);
4.4.4.8. A solução deverá possuir pelo menos dois perfis pré-configurados de fábrica para uso imediato e permitir a customização de um perfil;
4.4.4.9. 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;
4.4.4.10. 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;
4.4.4.11. 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.
4.4.4.12. Deve ser possível visualizar a lista de proteções disponíveis no equipamento com os detalhes.
4.4.4.13. 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 & control).
4.4.4.14. A solução deve bloquear arquivos potencialmente maliciosos infectados com malware.
4.4.4.15. A solução de proteção contra malware e bot deve compartilhar a mesma política para facilitar o gerenciamento.
4.4.4.16. 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;
4.4.4.17. As proteções devem ser ativadas baseadas em, pelo menos, critério de nível de confiança, ações da proteção e impacto de performance.
4.4.4.18. Deve ser possível habilitar a trilha das proteções para não logar, criar um log ou gerar um alerta;
4.4.4.19. 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.
4.4.4.20. A solução de anti-malware deve suportar protocolos SMTP e POP3, FTP, HTTP em qualquer porta;
4.4.4.21. Deve ser possível definir uma política de inspeção para os tipos de arquivos por:
4.4.4.21.1. Inspecionar tipos de arquivos conhecidos que contenham malware;
4.4.4.21.2. Inspecionar todos os tipos de arquivos;
4.4.4.21.3. Inspecionar tipos de arquivos de famílias específicas;
4.4.4.22. Deve bloquear acesso a URLs com malware;
4.4.4.23. Deve ser possível customizar a página exibida para o usuário quando a URL contiver um malware e o acesso for bloqueado;

4.4.5. PREVENÇÃO DE AMEAÇAS AVANÇADAS
4.4.5.1. 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.
4.4.5.2. A solução deve compartilhar a mesma política da proteção contra vírus e bot para facilitar o gerenciamento.
4.4.5.3. A solução deve trabalhar em modo de prevenção e não apenas detecção.

4.4.5.4. Deve permitir criar uma lista de exceção de e-mails que não devem ter seus anexos inspecionados.
4.4.5.5. Deve permitir criar uma lista de exceção para arquivos que não devem ser inspecionados.
4.4.5.6. A solução deve suportar protocolos SMTP, HTTP em qualquer porta;
4.4.5.7. Deve permitir configurar por tipo de arquivo as ações de inspeção ou bypass.
4.4.5.8. 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
4.4.5.9. Implementar detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF com tamanho até 15 Mb.
4.4.5.10. 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.

4.4.6. FILTRO DE CONTEÚDO WEB
4.4.6.1. 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;
4.4.6.2. A gerência das políticas de segurança de controle de aplicação e controle de URL's deverá ser realizada na mesma interface web de gerenciamento;
4.4.6.3. 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.
4.4.6.4. Deve ser possível configurar com apenas um clique o bloqueio a sites com conteúdo inapropriado como sexo, violência, armas, jogos e álcool.
4.4.6.5. Deve configurar regras para permitir ou bloquear aplicações ou páginas da Internet por pelo menos:
4.4.6.5.1. Usuário do Active Directory
4.4.6.5.2. IP
4.4.6.5.3. Rede
4.4.6.6. Deve ser possível configurar o bloqueio de compartilhamento de arquivos com origem usualmente ilegais como aplicações torrents e peer-to-peer.
4.4.6.7. Deve ser possível configurar manualmente o bloqueio de aplicações ou categorias de sites de aplicações indesejadas.
4.4.6.8. Deve ainda ser possível adicionar uma URL ou aplicação que não está na base de dados.
4.4.6.9. Deve ser possível limitar o consumo de banda de aplicações.
4.4.6.10. 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;
4.4.6.11. Deve ser possível realizar a recategorização de uma URL através da gerência do equipamento.
4.4.6.12. Deve ser possível customizar e definir a frequência com que serão exibidas as mensagens para os usuários nas seguintes ações:
4.4.6.12.1. Aceitar e informar
4.4.6.12.2. Bloquear e informar
4.4.6.12.3. Perguntar

4.4.7. IDENTIFICAÇÃO DE USUÁRIOS
4.4.7.1. A solução deve ser capaz de trabalhar com identidades de usuários para propósitos de configurações e logging.
4.4.7.2. A solução deve possibilitar ao administrador realizar a integração com o AD através de um assistente de configuração na própria interface gráfica do produto;
4.4.7.3. A solução deve identificar usuários das seguintes fontes:
4.4.7.3.1. Active Directory - o gateway de segurança deve realizar consulta aos servidores AD para obter informação dos usuários;
4.4.7.3.2. Autenticação via navegador - Para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador;

4.4.7.4. 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;
4.4.7.5. 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;

4.4.8. FUNCIONALIDADES DE ACESSO REMOTO
4.4.8.1. A solução deve prover acesso seguro encriptado aos usuários remotos através da Internet;
4.4.8.2. A solução deve prover conectividade através de um cliente instalado no computador do usuário e através do navegador do usuário com conexão segura (HTTPS).
4.4.8.3. Deve suportar pelo menos os seguintes métodos de conexão:
4.4.8.3.1. Conexão através de cliente instalado no laptop ou desktop do usuário.
4.4.8.3.2. Conexão através de cliente instalado no smartphone e tablets.
4.4.8.3.3. Conexão através de navegador com SSL.
4.4.8.3.4. Conexão através de cliente nativo Windows L2TP.
4.4.8.4. Solução deve suportar alterar a porta padrão 443 para estabelecimento de VPN SSL.
4.4.8.5. A solução deve permitir conexão VPN aos seguintes usuários:
4.4.8.5.1. Usuários locais na própria base do appliance.
4.4.8.5.2. Grupos de usuários locais na própria base do appliance.
4.4.8.5.3. Grupos de usuários do Active Directory.
4.4.8.5.4. Grupos de usuários Radius.
4.4.8.6. A solução deve permitir atribuir um endereço específico para o usuário remoto.

4.4.9. FUNCIONALIDADE DE VPN SITE-TO-SITE
4.4.9.1. A solução deve prover acesso seguro criptografado entre duas localidades através da Internet;
4.4.9.2. A solução deve estabelecer VPN com o site remoto do próprio fabricante ou de terceiros;
4.4.9.3. A solução deve suportar autenticação com senha ou certificado;
4.4.9.4. Deve suportar, pelo menos, criptografia AES 128 e 256;
4.4.9.5. Deve possuir mecanismo para monitorar a saúde do túnel remoto;
4.4.9.6. Quando o túnel for estabelecido entre dispositivos do mesmo fabricante este deve possuir protocolo proprietário para testar se o túnel está ativo.

4.5. ITEM 5 – NEXT GENERATION FIREWALL – SEDE TIPO I

4.5.1. CARACTERÍSTICAS GERAIS

4.5.1.1. É permitido a composição da solução ofertada entre diversos fabricantes, desde que não contemple solução de software livre;
4.5.1.2. A solução deverá ser compatível com SNMPv2 e SNMPv3;
4.5.1.3. 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;
4.5.1.4. A comunicação entre os appliances de segurança e o módulo de gerência deve ser através de meio criptografado;
4.5.1.5. Os appliances de segurança devem suportar operar em cluster ativo-ativo e ativo-passivo sem a necessidade de licenças adicionais;
4.5.1.6. Não serão aceitos modelos em listas de end-of-sale, cuja data do fim de vendas seja anterior à data da proposta.
4.5.1.7. 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.

4.5.2. CAPACIDADE E QUANTIDADES

4.5.2.1. 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;
4.5.2.2. Suporte a, no mínimo, 1.900.000 (um milhão e novecentas mil) conexões ou sessões simultâneas;
4.5.2.3. Suporte a, no mínimo, 30.000 (trinta mil) novas conexões ou sessões por segundo;
4.5.2.4. Throughput de, no mínimo, 2.5 Gbps (dois ponto cinco), para conexões VPN;
4.5.2.5. Armazenamento de, no mínimo, 200GB SSD;
4.5.2.6. No mínimo, 5 (cinco) interfaces de rede 1Gbps UTP;
4.5.2.7. 1 (uma) interface de rede dedicada ao gerenciamento;
4.5.2.8. 1 (uma) interface do tipo console ou similar;
4.5.2.9. 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.
4.5.2.10. 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;

4.5.3. FUNCIONALIDADE DE FIREWALL
4.5.3.1. A solução deve consistir de appliance de proteção de rede com funcionalidades de proteção de próxima geração;
4.5.3.2. 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;
4.5.3.3. 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;
4.5.3.4. Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19”, incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;
4.5.3.5. Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:
4.5.3.6. 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;
4.5.3.7. A solução deve possuir mecanismo onde identifica o volume de conexões que foi trafegada na regra, assim identificando as regras mais utilizadas;
4.5.3.8. Deve suportar os seguintes tipos de NAT:
4.5.3.9. 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;
4.5.3.10. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
4.5.3.11. Deve suportar NAT64 e NAT46;
4.5.3.12. Enviar logs para sistemas de monitoração externos, simultaneamente;
4.5.3.13. 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;
4.5.3.14. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
4.5.3.15. 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);
4.5.3.16. Para IPv6, deve suportar roteamento estático e dinâmico (OSPF);
4.5.3.17. Suportar OSPF graceful restart;
4.5.3.18. Autenticação integrada via Kerberos.
4.5.3.19. Cada regra deve, obrigatoriamente, funcionar nas versões de endereço IP 4 e 6 sem duplicação da base de objetos e regras;

4.5.3.20. Não serão aceitas soluções nas quais as interfaces de origem e destino tenham que ser obrigatoriamente explicitadas ou obrigatoriamente listadas nas configurações de regras;

4.5.4. FUNCIONALIDADE DE CONTROLE DE DADOS E FILTRO DE CONTEÚDO WEB

4.5.4.1. 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;
4.5.4.2. Controle de políticas por usuários, grupos de usuários, IPs e redes;
4.5.4.3. Deve de-criptografar tráfego de entrada e saída em conexões negociadas com TLS 1.2;
4.5.4.4. Será aceito soluções de outros fabricantes diferentes do firewall ofertado pela licitante desde que atendido todos os requisitos desta especificação;
4.5.4.5. Suportar a atribuição de agendamento às políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;
4.5.4.6. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:
4.5.4.7. Deve ser possível a liberação e bloqueio de aplicações sem a necessidade de liberação de portas e protocolos;
4.5.4.8. 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, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;
4.5.4.9. Para tráfego criptografado (SSL), deve de-criptografar pacotes a fim de possibilitar a leitura do payload para checagem de assinaturas de aplicações conhecidas;
4.5.4.10. A solução deve suportar a recategorização de URLs local;
4.5.4.11. Atualizar a base de assinaturas de aplicações automaticamente;
4.5.4.12. A solução deve permitir a solicitação da contratada com o fabricante para categorização de URL na base do fabricante;
4.5.4.13. Limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD;
4.5.4.14. 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 domínio, nem nas estações dos usuários;
4.5.4.15. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos ou análise heurística;
4.5.4.16. 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;
4.5.4.17. A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:
4.5.4.18. Permitir especificar política por tempo, com definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
4.5.4.19. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes;
4.5.4.20. Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;
4.5.4.21. 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;
4.5.4.22. 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;
4.5.4.23. Suportar a criação de categorias de URLs customizadas;
4.5.4.24. Permitir a customização de página de bloqueio;
4.5.4.25. Como melhor pratica do uso do acesso a internet e respeitando as politicas 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 estabelecidas pela area de TI;

4.5.4.26. 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;
4.5.4.27. 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);
4.5.4.28. 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:
4.5.4.28.1. PCI – números de cartão de crédito;
4.5.4.28.2. Arquivos PDF;
4.5.4.28.3. Arquivos executáveis;
4.5.4.28.4. Arquivos de banco de dados;
4.5.4.28.5. Arquivos do tipo documento;
4.5.4.28.6. Arquivos do tipo apresentação;
4.5.4.28.7. Arquivos do tipo planilha;
4.5.4.29. 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".
4.5.4.30. 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.
4.5.4.31. 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.

4.5.5. FUNCIONALIDADES DE PREVENÇÃO DE AMEAÇAS

4.5.5.1. 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;
4.5.5.2. Possuir capacidade de detecção de, no mínimo, 7.000 (sete mil) assinaturas de ataques pré-definidos;
4.5.5.3. A solução deve sincronizar ou aplicar as assinaturas de IPS, Antivírus, Anti-Malware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;
4.5.5.4. 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;
4.5.5.5. 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;
4.5.5.6. 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;
4.5.5.7. Detectar e bloquear a origem de portscans;
4.5.5.8. Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações;
4.5.5.9. A solução de IPS, deve suportar a inclusão de novas assinaturas e customização no formato SNORT;
4.5.5.10. Possuir assinaturas para bloqueio de ataques de buffer overflow;
4.5.5.11. Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP;
4.5.5.12. Suportar bloqueio de arquivos por tipo;
4.5.5.13. Identificar e bloquear comunicação com botnets;
4.5.5.14. Deve suportar referência cruzada com CVE;
4.5.5.15. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:
4.5.5.16. O nome da assinatura e do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo de proteção;
4.5.5.17. Deve suportar a captura de pacotes (PCAP), em assinatura de IPS e Anti-Malware, através da console de gerência centralizada;

4.5.5.18. Os eventos devem identificar o país de onde partiu a ameaça;
4.5.5.19. Deve suportar a inspeção em arquivos comprimidos (zip, gzip,etc.);
4.5.5.20. Possuir a capacidade de prevenção de ameaças não conhecidas;
4.5.5.21. Suportar a criação de políticas por Geo Localização, permitindo que o tráfego de determinado País/ Países seja bloqueado;
4.5.5.22. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
4.5.5.23. A solução de anti-malware, deve ser capaz de detectar e bloquear ações de callbacks;

4.5.6. FUNCIONALIDADES DE CONTROLE DE QUALIDADE DE SERVIÇO

4.5.6.1. Suportar a criação de políticas de QoS por:
4.5.6.2. Endereço de origem, endereço de destino e por porta;
4.5.6.3. O QoS deve possibilitar a definição de classes por:
4.5.6.3.1. Banda garantida;
4.5.6.3.2. Banda máxima ;
4.5.6.3.3. Fila de prioridade;
4.5.6.4. Disponibilizar estatísticas RealTime para classes de QoS;

4.5.7. FUNCIONALIDADES DE VPN

4.5.7.1. Suportar VPN Site-to-Site e Cliente-To-Site;
4.5.7.2. Suportar IPSec VPN;
4.5.7.3. Suportar SSL VPN;
4.5.7.4. A VPN IPSEc deve suportar:
4.5.7.4.1. 3DES, Autenticação MD5 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;
4.5.7.5. A solução deve suportar CA Interna e CA Externa de terceiros;
4.5.7.6. Solução deve suportar a configuração VPN através de uma interface do tipo GUI (console do fabricante ou interface web);

4.5.8. SOLUÇÃO DE PROTEÇÃO CONTRA AMEAÇAS AVANÇADAS

4.5.8.1. 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 próprio fabricante ou appliance dedicada para sandboxing;
4.5.8.2. 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.
4.5.8.3. A solução deve ser capaz de inspecionar e prevenir malware desconhecido em tráfego criptografado SSL;
4.5.8.4. 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;
4.5.8.5. 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;
4.5.8.6. A solução deve suportar as seguintes topologias de implantação: Inline, Message Transfer Agent (MTA) e Mirror/TAP;
4.5.8.7. 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;

4.5.8.8. A solução de prevença de ameaças avançadas (Sandboxing) contra ataques persistentes e Zero-Day, 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.
4.5.8.9. 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;
4.5.8.10. Para a emulação de arquivos, a solução deve suportar arquivos com tamanho máximo de emulação de até 30Mb.
4.5.8.11. Implementar mecanismo de exceção, permitindo a criação de regras por VLAN, subrede e endereço IP;
4.5.8.12. 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, scr, xls, xlsx, xlt, xlm, xltx, xlsm, xltm, xlsb, xla, xlam, xll, xlw, ppt, pptx, pps, pptm, potx, potm, ppam, ppsx, ppsm, doc, docx, dot, docm, dotx, dotm;
4.5.8.13. A solução deve permitir a criação de Whitelists baseado no MD5 do arquivo;
4.5.8.14. Para melhor administração da solução, a solução deve possibilitar as seguintes visualizações a nível de monitoração:
4.5.8.14.1. Quantidade de arquivos que estão em emulação;
4.5.8.14.2. Número de arquivos emulados;
4.5.8.15. A solução deve possuir os indicadores abaixo referente ao último dia, última semana ou últimos 30 dias:
4.5.8.15.1. Arquivos scaneados;
4.5.8.15.2. Arquivos maliciosos;

4.6. ITEM 6 – NEXT GENERATION FIREWALL – SEDE TIPO II

4.6.1. CARACTERÍSTICAS GERAIS

4.6.1.1. É permitido a composição da solução ofertada entre diversos fabricantes, desde que não contemple solução de software livre;
4.6.1.2. A solução deverá ser compatível com SNMPv2 e SNMPv3;
4.6.1.3. 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;
4.6.1.4. A comunicação entre os appliances de segurança e o módulo de gerência deve ser através de meio criptografado;
4.6.1.5. Os appliances de segurança devem suportar operar em cluster ativo-ativo e ativo-passivo sem a necessidade de licenças adicionais;
4.6.1.6. Não serão aceitos modelos em listas de end-of-sale, cuja data do fim de vendas seja anterior à data da proposta.
4.6.1.7. 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.

4.6.2. CAPACIDADE E QUANTIDADES

4.6.2.1. Throughput de, no mínimo, 1.7 Gbps, com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação, anti-malware e prevenção de ameaças avançadas (dia zero) habilitados simultaneamente;
4.6.2.2. Suporte a, no mínimo, 3.900.000 (três milhões e novecentas mil) conexões ou sessões simultâneas;
4.6.2.3. Suporte a, no mínimo, 65.000 (sessenta e cinco mil) novas conexões ou sessões por segundo;
4.6.2.4. Throughput de, no mínimo, 2.5 Gbps (dois ponto cinco), para conexões VPN;
4.6.2.5. Armazenamento de, no mínimo, 200GB SSD;
4.6.2.6. Possuir, no mínimo, 8 (oito) interfaces de rede 1Gbps UTP;

4.6.2.7. Possuir, no mínimo, 4 (quatro) interfaces de rede 1 Gbps SFP;
4.6.2.8. Capacidade para suportar, pelo menos, 20 contextos virtuais;
4.6.2.9. Possuir fonte de alimentação redundante;
4.6.2.10. Possuir 1 (uma) interface de rede dedicada ao gerenciamento;
4.6.2.11. Possuir 1 (uma) interface de rede dedicada para sincronismo;
4.6.2.12. Possuir 1 (uma) interface do tipo console ou similar;
4.6.2.13. 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 fisica/dedicada, deverá ser composta com outro equipamento de terceiro onde faça essa função. Não sendo permitido qualquer tipo de configuração de instâncias via software.
4.6.2.14. 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.
4.6.2.15. 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;
4.6.2.16. Todas as interfaces fornecidas nos appliances devem estar licenciadas e habilitadas para uso imediato, incluindo seus transceivers/transceptores. Caso sejam fornecidas interfaces além das exigidas, todas as interfaces devem ser fornecidas com todos os transceivers/transceptores necessários para a plena utilização;

4.6.3. FUNCIONALIDADE DE FIREWALL
4.6.3.1. A solução deve consistir de appliance de proteção de rede com funcionalidades de proteção de próxima geração;
4.6.3.2. 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;
4.6.3.3. 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;
4.6.3.4. Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19”, incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;
4.6.3.5. Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:
4.6.3.6. 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;
4.6.3.7. A solução deve possuir mecanismo onde identifica o volume de conexões que foi trafegada na regra, assim identificando as regras mais utilizadas;
4.6.3.8. Deve suportar os seguintes tipos de NAT:
4.6.3.9. 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;
4.6.3.10. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
4.6.3.11. Deve suportar NAT64 e NAT46;
4.6.3.12. Enviar logs para sistemas de monitoração externos, simultaneamente;
4.6.3.13. 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;
4.6.3.14. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
4.6.3.15. 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);
4.6.3.16. Para IPv6, deve suportar roteamento estático e dinâmico (OSPF);
4.6.3.17. Suportar OSPF graceful restart;

4.6.3.18. Autenticação integrada via Kerberos.
4.6.3.19. Cada regra deve, obrigatoriamente, funcionar nas versões de endereço IP 4 e 6 sem duplicação da base de objetos e regras;
4.6.3.20. Não serão aceitas soluções nas quais as interfaces de origem e destino tenham que ser obrigatoriamente explicitadas ou obrigatoriamente listadas nas configurações de regras;

4.6.4. FUNCIONALIDADE DE CONTROLE DE DADOS E FILTRO DE CONTEÚDO WEB

4.6.4.1. 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;
4.6.4.2. Controle de políticas por usuários, grupos de usuários, IPs e redes;
4.6.4.3. Deve de-criptografar tráfego de entrada e saída em conexões negociadas com TLS 1.2;
4.6.4.4. Será aceito soluções de outros fabricantes diferentes do firewall ofertado pela licitante desde que atendido todos os requisitos desta especificação;
4.6.4.5. Suportar a atribuição de agendamento às políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;
4.6.4.6. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:
4.6.4.7. Deve ser possível a liberação e bloqueio de aplicações sem a necessidade de liberação de portas e protocolos;
4.6.4.8. 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;
4.6.4.9. Para tráfego criptografado (SSL), deve de-criptografar pacotes a fim de possibilitar a leitura do payload para checagem de assinaturas de aplicações conhecidas;
4.6.4.10. A solução deve suportar a recategorização de URLs local;
4.6.4.11. Atualizar a base de assinaturas de aplicações automaticamente;
4.6.4.12. A solução deve permitir a solicitação da contratada com o fabricante para categorização de URL na base do fabricante;
4.6.4.13. Limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD;
4.6.4.14. 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;
4.6.4.15. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos ou análise heurística;
4.6.4.16. 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;
4.6.4.17. A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:
4.6.4.18. Permitir especificar política por tempo, com definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
4.6.4.19. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes;
4.6.4.20. Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;
4.6.4.21. 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;
4.6.4.22. 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;
4.6.4.23. Suportar a criação de categorias de URLs customizadas;
4.6.4.24. Permitir a customização de página de bloqueio;

4.6.4.25. 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;
4.6.4.26. 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;
4.6.4.27. 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);
4.6.4.28. 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:
4.6.4.28.1. PCI – números de cartão de crédito;
4.6.4.28.2. Arquivos PDF;
4.6.4.28.3. Arquivos executáveis;
4.6.4.28.4. Arquivos de banco de dados;
4.6.4.28.5. Arquivos do tipo documento;
4.6.4.28.6. Arquivos do tipo apresentação;
4.6.4.28.7. Arquivos do tipo planilha;
4.6.4.29. 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".
4.6.4.30. 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.
4.6.4.31. 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.

4.6.5. FUNCIONALIDADES DE PREVENÇÃO DE AMEAÇAS

4.6.5.1. 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;
4.6.5.2. Possuir capacidade de detecção de, no mínimo, 7.000 (sete mil) assinaturas de ataques pré-definidos;
4.6.5.3. A solução deve sincronizar ou aplicar as assinaturas de IPS, Antivírus, Anti-Malware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;
4.6.5.4. 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;
4.6.5.5. 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;
4.6.5.6. 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;
4.6.5.7. Detectar e bloquear a origem de portscans;
4.6.5.8. Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações;
4.6.5.9. A solução de IPS, deve suportar a inclusão de novas assinaturas e customização no formato SNORT;
4.6.5.10. Possuir assinaturas para bloqueio de ataques de buffer overflow;
4.6.5.11. Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP;
4.6.5.12. Suportar bloqueio de arquivos por tipo;
4.6.5.13. Identificar e bloquear comunicação com botnets;
4.6.5.14. Deve suportar referência cruzada com CVE;
4.6.5.15. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:

4.6.5.16. O nome da assinatura e do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo de proteção;
4.6.5.17. Deve suportar a captura de pacotes (PCAP), em assinatura de IPS e Anti-Malware, através da console de gerência centralizada;
4.6.5.18. Os eventos devem identificar o país de onde partiu a ameaça;
4.6.5.19. Deve suportar a inspeção em arquivos comprimidos (zip, gzip,etc.);
4.6.5.20. Possuir a capacidade de prevenção de ameaças não conhecidas;
4.6.5.21. Suportar a criação de políticas por Geo Localização, permitindo que o tráfego de determinado País/ Países seja bloqueado;
4.6.5.22. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
4.6.5.23. A solução de anti-malware, deve ser capaz de detectar e bloquear ações de callbacks;

4.6.6. FUNCIONALIDADES DE CONTROLE DE QUALIDADE DE SERVIÇO

4.6.6.1. Suportar a criação de políticas de QoS por:
4.6.6.2. Endereço de origem, endereço de destino e por porta;
4.6.6.3. O QoS deve possibilitar a definição de classes por:
4.6.6.3.1. Banda garantida;
4.6.6.3.2. Banda máxima ;
4.6.6.3.3. Fila de prioridade;
4.6.6.4. Disponibilizar estatísticas RealTime para classes de QoS;

4.6.7. FUNCIONALIDADES DE VPN

4.6.7.1. Suportar VPN Site-to-Site e Cliente-To-Site;
4.6.7.2. Suportar IPSec VPN;
4.6.7.3. Suportar SSL VPN;
4.6.7.4. A VPN IPSEc deve suportar:
4.6.7.4.1. 3DES, Autenticação MD5 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;
4.6.7.5. A solução deve suportar CA Interna e CA Externa de terceiros;
4.6.7.6. Solução deve suportar a configuração VPN através de uma interface do tipo GUI (console do fabricante ou interface web);

4.6.8. SOLUÇÃO DE PROTEÇÃO CONTRA AMEAÇAS AVANÇADAS

4.6.8.1. 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 da próprio fabricante ou appliance dedicada para sandboxing;
4.6.8.2. 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.
4.6.8.3. A solução deve ser capaz de inspecionar e prevenir malware desconhecido em tráfego criptografado SSL;
4.6.8.4. 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;
4.6.8.5. 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;
4.6.8.6. A solução deve suportar as seguintes topologias de implantação: Inline, Message Transfer Agent (MTA) e Mirror/TAP;

4.6.8.7. 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;
4.6.8.8. A solução de prevença de ameaças avançadas (Sandboxing) contra ataques persistentes e Zero-Day, 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.
4.6.8.9. 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;
4.6.8.10. Para a emulação de arquivos, a solução deve suportar arquivos com tamanho máximo de emulação de até 30Mb.
4.6.8.11. Implementar mecanismo de exceção, permitindo a criação de regras por VLAN, subrede e endereço IP;
4.6.8.12. 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, scr, xls, xlsx, xlt, xlm, xltx, xlsm, xltm, xlsb, xla, xlam, xll, xlw, ppt, pptx, pps, pptm, potx, potm, ppam, ppsx, ppsm, doc, docx, dot, docm, dotx, dotm;
4.6.8.13. A solução deve permitir a criação de Whitelists baseado no MD5 do arquivo;
4.6.8.14. Para melhor administração da solução, a solução deve possibilitar as seguintes visualizações a nível de monitoração:
4.6.8.14.1. Quantidade de arquivos que estão em emulação;
4.6.8.14.2. Número de arquivos emulados;
4.6.8.15. A solução deve possuir os indicadores abaixo referente ao último dia, última semana ou últimos 30 dias:
4.6.8.15.1. Arquivos scaneados;
4.6.8.15.2. Arquivos maliciosos;

4.7. ITEM 7 – NEXT GENERATION FIREWALL – SEDE TIPO III

4.7.1. CARACTERÍSTICAS GERAIS

4.7.1.1. É permitido a composição da solução ofertada entre diversos fabricantes, desde que não contemple solução de software livre;
4.7.1.2. A solução deverá ser compatível com SNMPv2 e SNMPv3;
4.7.1.3. 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;
4.7.1.4. A comunicação entre os appliances de segurança e o módulo de gerência deve ser através de meio criptografado;
4.7.1.5. Os appliances de segurança devem suportar operar em cluster ativo-ativo e ativo-passivo sem a necessidade de licenças adicionais;
4.7.1.6. Não serão aceitos modelos em listas de end-of-sale, cuja data do fim de vendas seja anterior à data da proposta.
4.7.1.7. 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.

4.7.2. CAPACIDADE E QUANTIDADES

4.7.2.1. Throughput de, no mínimo, 3.6 Gbps, com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação, anti-malware e prevenção de ameaças avançadas (dia zero) habilitados simultaneamente;
4.7.2.2. Suporte a, no mínimo, 3.900.000 (três milhões e novecentas mil) conexões ou sessões simultâneas;
4.7.2.3. Suporte a, no mínimo, 115.000 (cento e quinze mil) novas conexões ou sessões por segundo;

4.7.2.4. Throughput de, no mínimo, 4.7 Gbps (quatro ponto sete), para conexões VPN;
4.7.2.5. Armazenamento de, no mínimo, 200GB SSD;
4.7.2.6. Possuir, no mínimo, 8 (oito) interfaces de rede 1Gbps UTP;
4.7.2.7. Possuir, no mínimo, 4 (quatro) interfaces de rede 10 Gbps SFP+;
4.7.2.8. Capacidade para suportar, pelo menos, 20 contextos virtuais;
4.7.2.9. Possuir fonte de alimentação redundante e hot-swappable;
4.7.2.10. Possuir 1 (uma) interface de rede dedicada ao gerenciamento;
4.7.2.11. Possuir 1 (uma) interface de rede dedicada para sincronismo;
4.7.2.12. Possuir 1 (uma) interface do tipo console ou similar;
4.7.2.13. 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 fisica/dedicada, deverá ser composta com outro equipamento de terceiro onde faça essa função. Não sendo permitido qualquer tipo de configuração de instancias via software.
4.7.2.14. 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.
4.7.2.15. 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;
4.7.2.16. Todas as interfaces fornecidas nos appliances devem estar licenciadas e habilitadas para uso imediato, incluindo seus transceivers/transceptores. Caso sejam fornecidas interfaces além das exigidas, todas as interfaces devem ser fornecidas com todos os transceivers/transceptores necessários para a plena utilização;

4.7.3. FUNCIONALIDADE DE FIREWALL
4.7.3.1. A solução deve consistir de appliance de proteção de rede com funcionalidades de proteção de próxima geração;
4.7.3.2. 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;
4.7.3.3. 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;
4.7.3.4. Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19”, incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;
4.7.3.5. Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:
4.7.3.6. 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;
4.7.3.7. A solução deve possuir mecanismo onde identifica o volume de conexões que foi trafegada na regra, assim identificando as regras mais utilizadas;
4.7.3.8. Deve suportar os seguintes tipos de NAT:
4.7.3.9. 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;
4.7.3.10. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
4.7.3.11. Deve suportar NAT64 e NAT46;
4.7.3.12. Enviar logs para sistemas de monitoração externos, simultaneamente;
4.7.3.13. 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;
4.7.3.14. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);

4.7.3.15. 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);
4.7.3.16. Para IPv6, deve suportar roteamento estático e dinâmico (OSPF);
4.7.3.17. Suportar OSPF graceful restart;
4.7.3.18. Autenticação integrada via Kerberos.
4.7.3.19. Cada regra deve, obrigatoriamente, funcionar nas versões de endereço IP 4 e 6 sem duplicação da base de objetos e regras;
4.7.3.20. Não serão aceitas soluções nas quais as interfaces de origem e destino tenham que ser obrigatoriamente explicitadas ou obrigatoriamente listadas nas configurações de regras;

4.7.4. FUNCIONALIDADE DE CONTROLE DE DADOS E FILTRO DE CONTEÚDO WEB

4.7.4.1. 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;
4.7.4.2. Controle de políticas por usuários, grupos de usuários, IPs e redes;
4.7.4.3. Deve de-criptografar tráfego de entrada e saída em conexões negociadas com TLS 1.2;
4.7.4.4. Será aceito soluções de outros fabricantes diferentes do firewall ofertado pela licitante desde que atendido todos os requisitos desta especificação;
4.7.4.5. Suportar a atribuição de agendamento às políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;
4.7.4.6. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:
4.7.4.7. Deve ser possível a liberação e bloqueio de aplicações sem a necessidade de liberação de portas e protocolos;
4.7.4.8. 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;
4.7.4.9. Para tráfego criptografado (SSL), deve de-criptografar pacotes a fim de possibilitar a leitura do payload para checagem de assinaturas de aplicações conhecidas;
4.7.4.10. A solução deve suportar a recategorização de URLs local;
4.7.4.11. Atualizar a base de assinaturas de aplicações automaticamente;
4.7.4.12. A solução deve permitir a solicitação da contratada com o fabricante para categorização de URL na base do fabricante;
4.7.4.13. Limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD;
4.7.4.14. 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;
4.7.4.15. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos ou análise heurística;
4.7.4.16. 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;
4.7.4.17. A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:
4.7.4.18. Permitir especificar política por tempo, com definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
4.7.4.19. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes;
4.7.4.20. Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;
4.7.4.21. 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;

4.7.4.22. 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;
4.7.4.23. Suportar a criação de categorias de URLs customizadas;
4.7.4.24. Permitir a customização de página de bloqueio;
4.7.4.25. 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;
4.7.4.26. 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;
4.7.4.27. 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 Firewall (Captive Portal);
4.7.4.28. 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:
4.7.4.28.1. PCI – números de cartão de crédito;
4.7.4.28.2. Arquivos PDF;
4.7.4.28.3. Arquivos executáveis;
4.7.4.28.4. Arquivos de banco de dados;
4.7.4.28.5. Arquivos do tipo documento;
4.7.4.28.6. Arquivos do tipo apresentação;
4.7.4.28.7. Arquivos do tipo planilha;
4.7.4.29. 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".
4.7.4.30. 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.
4.7.4.31. 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.

4.7.5. FUNCIONALIDADES DE PREVENÇÃO DE AMEAÇAS

4.7.5.1. 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;
4.7.5.2. Possuir capacidade de detecção de, no mínimo, 7.000 (sete mil) assinaturas de ataques pré-definidos;
4.7.5.3. A solução deve sincronizar ou aplicar as assinaturas de IPS, Antivírus, Anti-Malware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;
4.7.5.4. 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;
4.7.5.5. 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;
4.7.5.6. 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;
4.7.5.7. Detectar e bloquear a origem de portscans;
4.7.5.8. Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações;
4.7.5.9. A solução de IPS, deve suportar a inclusão de novas assinaturas e customização no formato SNORT;
4.7.5.10. Possuir assinaturas para bloqueio de ataques de buffer overflow;

4.7.5.11. Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP;
4.7.5.12. Suportar bloqueio de arquivos por tipo;
4.7.5.13. Identificar e bloquear comunicação com botnets;
4.7.5.14. Deve suportar referência cruzada com CVE;
4.7.5.15. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:
4.7.5.16. O nome da assinatura e do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo de proteção;
4.7.5.17. Deve suportar a captura de pacotes (PCAP), em assinatura de IPS e Anti-Malware, através da console de gerência centralizada;
4.7.5.18. Os eventos devem identificar o país de onde partiu a ameaça;
4.7.5.19. Deve suportar a inspeção em arquivos comprimidos (zip, gzip,etc.);
4.7.5.20. Possuir a capacidade de prevenção de ameaças não conhecidas;
4.7.5.21. Suportar a criação de políticas por Geo Localização, permitindo que o tráfego de determinado País/Países seja bloqueado;
4.7.5.22. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
4.7.5.23. A solução de anti-malware, deve ser capaz de detectar e bloquear ações de callbacks;

4.7.6. FUNCIONALIDADES DE CONTROLE DE QUALIDADE DE SERVIÇO
4.7.6.1. Suportar a criação de políticas de QoS por:
4.7.6.2. Endereço de origem, endereço de destino e por porta;
4.7.6.3. O QoS deve possibilitar a definição de classes por:
4.7.6.3.1. Banda garantida;
4.7.6.3.2. Banda máxima ;
4.7.6.3.3. Fila de prioridade;
4.7.6.4. Disponibilizar estatísticas RealTime para classes de QoS;

4.7.7. FUNCIONALIDADES DE VPN
4.7.7.1. Suportar VPN Site-to-Site e Cliente-To-Site;
4.7.7.2. Suportar IPSec VPN;
4.7.7.3. Suportar SSL VPN;
4.7.7.4. A VPN IPSEc deve suportar:
4.7.7.4.1. 3DES, Autenticação MD5 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;
4.7.7.5. A solução deve suportar CA Interna e CA Externa de terceiros;
4.7.7.6. Solução deve suportar a configuração VPN através de uma interface do tipo GUI (console do fabricante ou interface web);

4.7.8. SOLUÇÃO DE PROTEÇÃO CONTRA AMEAÇAS AVANÇADAS
4.7.8.1. 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;
4.7.8.2. 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.
4.7.8.3. A solução deve ser capaz de inspecionar e prevenir malware desconhecido em tráfego criptografado SSL;
4.7.8.4. 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;
4.7.8.5. 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;
4.7.8.6. A solução deve suportar as seguintes topologias de implantação: Inline, Message Transfer Agent (MTA) e Mirror/TAP;

4.7.8.7. 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;
4.7.8.8. A solução de prevenção de ameaças avançadas (Sandboxing) contra ataques persistentes e Zero-Day, 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.
4.7.8.9. 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;
4.7.8.10. Para a emulação de arquivos, a solução deve suportar arquivos com tamanho máximo de emulação de até 30Mb.
4.7.8.11. Implementar mecanismo de exceção, permitindo a criação de regras por VLAN, subrede e endereço IP;
4.7.8.12. 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, scr, xls, xlsx, xlt, xlm, xltx, xlsm, xltm, xlsb, xla, xlam, xll, xlw, ppt, pptx, pps, pptm, potx, potm, ppam, ppsx, ppsm, doc, docx, dot, docm, dotx, dotm;
4.7.8.13. A solução deve permitir a criação de Whitelists baseado no MD5 do arquivo;
4.7.8.14. Para melhor administração da solução, a solução deve possibilitar as seguintes visualizações a nível de monitoração:
4.7.8.14.1. Quantidade de arquivos que estão em emulação;
4.7.8.14.2. Número de arquivos emulados;
4.7.8.15. A solução deve possuir os indicadores abaixo referente ao último dia, última semana ou últimos 30 dias:
4.7.8.15.1. Arquivos scaneados;
4.7.8.15.2. Arquivos maliciosos;

4.8. ITEM 8 – NEXT GENERATION FIREWALL – DATA CENTER TIPO I

4.8.1. CARACTERÍSTICAS GERAIS

4.8.1.1. É permitido a composição da solução ofertada entre diversos fabricantes, desde que não contemple solução de software livre;
4.8.1.2. A solução deverá ser compatível com SNMPv2 e SNMPv3;
4.8.1.3. 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;
4.8.1.4. A comunicação entre os appliances de segurança e o módulo de gerência deve ser através de meio criptografado;
4.8.1.5. Os appliances de segurança devem suportar operar em cluster ativo-ativo e ativo-passivo sem a necessidade de licenças adicionais;
4.8.1.6. Não serão aceitos modelos em listas de end-of-sale, cuja data do fim de vendas seja anterior à data da proposta.
4.8.1.7. 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.

4.8.2. CAPACIDADE E QUANTIDADES
4.8.2.1. Throughput de, no mínimo, 9.3 Gbps, com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação, anti-malware e prevenção de ameaças avançadas (dia zero) habilitados simultaneamente;
4.8.2.2. Suporte a, no mínimo, 7.900.000 (sete milhões e novecentas mil) conexões ou sessões simultâneas;
4.8.2.3. Suporte a, no mínimo, 325.000 (trezentos e vinte e cinco mil) novas conexões ou sessões por segundo;

4.8.2.4. Throughput de, no mínimo, 11.5 Gbps (onze ponto cinco), para conexões VPN;
4.8.2.5. Armazenamento redundante de, no mínimo, 200 GB SSD ou HDD;
4.8.2.6. Possuir, no mínimo, 8 (oito) interfaces de rede 1Gbps UTP;
4.8.2.7. Possuir, no mínimo, 4 (quatro) interfaces de rede 10 Gbps SFP+;
4.8.2.8. Suportar expansão para, no mínimo, 2 interfaces de rede 40Gbps QSFP+;
4.8.2.9. Capacidade para suportar, pelo menos, 20 contextos virtuais;
4.8.2.10. Possuir fonte de alimentação redundante e hot-swappable;
4.8.2.11. Possuir 1 (uma) interface de rede dedicada ao gerenciamento;
4.8.2.12. Possuir 1 (uma) interface de rede dedicada para sincronismo;
4.8.2.13. Possuir 1 (uma) interface do tipo console ou similar;
4.8.2.14. 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 fisica/dedicada, deverá ser composta com outro equipamento de terceiro onde faça essa função. Não sendo permitido qualquer tipo de configuração de instancias via software.
4.8.2.15. 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.
4.8.2.16. 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;
4.8.2.17. Todas as interfaces fornecidas nos appliances devem estar licenciadas e habilitadas para uso imediato, incluindo seus transceivers/transceptores. Caso sejam fornecidas interfaces além das exigidas, todas as interfaces devem ser fornecidas com todos os transceivers/transceptores necessários para a plena utilização;

4.8.3. FUNCIONALIDADE DE FIREWALL
4.8.3.1. A solução deve consistir de appliance de proteção de rede com funcionalidades de proteção de próxima geração;
4.8.3.2. 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;
4.8.3.3. 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;
4.8.3.4. Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19”, incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;
4.8.3.5. Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:
4.8.3.6. 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;
4.8.3.7. A solução deve possuir mecanismo onde identifica o volume de conexões que foi trafegada na regra, assim identificando as regras mais utilizadas;
4.8.3.8. Deve suportar os seguintes tipos de NAT:
4.8.3.9. 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;
4.8.3.10. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
4.8.3.11. Deve suportar NAT64 e NAT46;
4.8.3.12. Enviar logs para sistemas de monitoração externos, simultaneamente;
4.8.3.13. 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;
4.8.3.14. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);

4.8.3.15. 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 (monitoramento e análise o tráfego de rede), camada 2 (L2) e camada 3 (L3);
4.8.3.16. Para IPv6, deve suportar roteamento estático e dinâmico (OSPF);
4.8.3.17. Suportar OSPF graceful restart;
4.8.3.18. Autenticação integrada via Kerberos.
4.8.3.19. Cada regra deve, obrigatoriamente, funcionar nas versões de endereço IP 4 e 6 sem duplicação da base de objetos e regras;
4.8.3.20. Não serão aceitas soluções nas quais as interfaces de origem e destino tenham que ser obrigatoriamente explicitadas ou obrigatoriamente listadas nas configurações de regras;

4.8.4. FUNCIONALIDADE DE CONTROLE DE DADOS E FILTRO DE CONTEÚDO WEB
4.8.4.1. 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;
4.8.4.2. Controle de políticas por usuários, grupos de usuários, IPs e redes;
4.8.4.3. Deve de-criptografar tráfego de entrada e saída em conexões negociadas com TLS 1.2;
4.8.4.4. Será aceito soluções de outros fabricantes diferentes do firewall ofertado pela licitante desde que atendido todos os requisitos desta especificação;
4.8.4.5. Suportar a atribuição de agendamento às políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;
4.8.4.6. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:
4.8.4.7. Deve ser possível a liberação e bloqueio de aplicações sem a necessidade de liberação de portas e protocolos;
4.8.4.8. 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;
4.8.4.9. Para tráfego criptografado (SSL), deve de-criptografar pacotes a fim de possibilitar a leitura do payload para checagem de assinaturas de aplicações conhecidas;
4.8.4.10. A solução deve suportar a recategorização de URLs local;
4.8.4.11. Atualizar a base de assinaturas de aplicações automaticamente;
4.8.4.12. A solução deve permitir a solicitação da contratada com o fabricante para categorização de URL na base do fabricante;
4.8.4.13. Limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD;
4.8.4.14. 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;
4.8.4.15. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos ou análise heurística;
4.8.4.16. 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;
4.8.4.17. A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:
4.8.4.18. Permitir especificar política por tempo, com definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
4.8.4.19. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes;
4.8.4.20. Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;
4.8.4.21. 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;
4.8.4.22. 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;

4.8.4.23. Suportar a criação de categorias de URLs customizadas;
4.8.4.24. Permitir a customização de página de bloqueio;
4.8.4.25. 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;
4.8.4.26. 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;
4.8.4.27. 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);
4.8.4.28. 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:
4.8.4.28.1. PCI – números de cartão de crédito;
4.8.4.28.2. Arquivos PDF;
4.8.4.28.3. Arquivos executáveis;
4.8.4.28.4. Arquivos de banco de dados;
4.8.4.28.5. Arquivos do tipo documento;
4.8.4.28.6. Arquivos do tipo apresentação;
4.8.4.28.7. Arquivos do tipo planilha;
4.8.4.29. 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".
4.8.4.30. 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.
4.8.4.31. 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.

4.8.5. FUNCIONALIDADES DE PREVENÇÃO DE AMEAÇAS
4.8.5.1. 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;
4.8.5.2. Possuir capacidade de detecção de, no mínimo, 7.000 (sete mil) assinaturas de ataques pré-definidos;
4.8.5.3. A solução deve sincronizar ou aplicar as assinaturas de IPS, Antivírus, Anti-Malware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;
4.8.5.4. 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;
4.8.5.5. 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;
4.8.5.6. 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;
4.8.5.7. Detectar e bloquear a origem de portscans;
4.8.5.8. Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações;
4.8.5.9. A solução de IPS, deve suportar a inclusão de novas assinaturas e customização no formato SNORT;
4.8.5.10. Possuir assinaturas para bloqueio de ataques de buffer overflow;
4.8.5.11. Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP;
4.8.5.12. Suportar bloqueio de arquivos por tipo;
4.8.5.13. Identificar e bloquear comunicação com botnets;

4.8.5.14. Deve suportar referência cruzada com CVE;
4.8.5.15. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:
4.8.5.16. O nome da assinatura e do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo de proteção;
4.8.5.17. Deve suportar a captura de pacotes (PCAP), em assinatura de IPS e Anti-Malware, através da console de gerência centralizada;
4.8.5.18. Os eventos devem identificar o país de onde partiu a ameaça;
4.8.5.19. Deve suportar a inspeção em arquivos comprimidos (zip, gzip,etc.);
4.8.5.20. Possuir a capacidade de prevenção de ameaças não conhecidas;
4.8.5.21. Suportar a criação de políticas por Geo Localização, permitindo que o tráfego de determinado País/Países seja bloqueado;
4.8.5.22. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
4.8.5.23. A solução de anti-malware, deve ser capaz de detectar e bloquear ações de callbacks;

4.8.6. FUNCIONALIDADES DE CONTROLE DE QUALIDADE DE SERVIÇO

4.8.6.1. Suportar a criação de políticas de QoS por:
4.8.6.2. Endereço de origem, endereço de destino e por porta;
4.8.6.3. O QoS deve possibilitar a definição de classes por:
4.8.6.3.1. Banda garantida;
4.8.6.3.2. Banda máxima ;
4.8.6.3.3. Fila de prioridade;
4.8.6.4. Disponibilizar estatísticas RealTime para classes de QoS;

4.8.7. FUNCIONALIDADES DE VPN

4.8.7.1. Suportar VPN Site-to-Site e Cliente-To-Site;
4.8.7.2. Suportar IPSec VPN;
4.8.7.3. Suportar SSL VPN;
4.8.7.4. A VPN IPSEc deve suportar:
4.8.7.4.1. 3DES, Autenticação MD5 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;
4.8.7.5. A solução deve suportar CA Interna e CA Externa de terceiros;
4.8.7.6. Solução deve suportar a configuração VPN através de uma interface do tipo GUI (console do fabricante ou interface web);

4.8.8. SOLUÇÃO DE PROTEÇÃO CONTRA AMEAÇAS AVANÇADAS

4.8.8.1. 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;
4.8.8.2. 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.
4.8.8.3. A solução deve ser capaz de inspecionar e prevenir malware desconhecido em tráfego criptografado SSL;
4.8.8.4. 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;
4.8.8.5. 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;
4.8.8.6. A solução deve suportar as seguintes topologias de implantação: Inline, Message Transfer Agent (MTA) e Mirror/TAP;

4.8.8.7. 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;
4.8.8.8. A solução de prevença de ameaças avançadas (Sandboxing) contra ataques persistentes e Zero-Day, 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.
4.8.8.9. 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;
4.8.8.10. Para a emulação de arquivos, a solução deve suportar arquivos com tamanho máximo de emulação de até 30Mb.
4.8.8.11. Implementar mecanismo de exceção, permitindo a criação de regras por VLAN, subrede e endereço IP;
4.8.8.12. 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, scr, xls, xlsx, xlt, xlm, xltx, xlsm, xltm, xlsb, xla, xlam, xll, xlw, ppt, pptx, pps, pptm, potx, potm, ppam, ppsx, ppsm, doc, docx, dot, docm, dotx, dotm;
4.8.8.13. A solução deve permitir a criação de Whitelists baseado no MD5 do arquivo;
4.8.8.14. Para melhor administração da solução, a solução deve possibilitar as seguintes visualizações a nível de monitoração:
4.8.8.14.1. Quantidade de arquivos que estão em emulação;
4.8.8.14.2. Número de arquivos emulados;
4.8.8.15. A solução deve possuir os indicadores abaixo referente ao último dia, última semana ou últimos 30 dias:
4.8.8.15.1. Arquivos scaneados;
4.8.8.15.2. Arquivos maliciosos;

4.9. ITEM 9 – NEXT GENERATION FIREWALL – DATA CENTER TIPO II

4.9.1. CARACTERÍSTICAS GERAIS

4.9.1.1. É permitido a composição da solução ofertada entre diversos fabricantes, desde que não contemple solução de software livre;
4.9.1.2. A solução deverá ser compatível com SNMPv2 e SNMPv3;
4.9.1.3. 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;
4.9.1.4. A comunicação entre os appliances de segurança e o módulo de gerência deve ser através de meio criptografado;
4.9.1.5. Os appliances de segurança devem suportar operar em cluster ativo-ativo e ativo-passivo sem a necessidade de licenças adicionais;
4.9.1.6. Não serão aceitos modelos em listas de end-of-sale, cuja data do fim de vendas seja anterior à data da proposta.
4.9.1.7. 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.

4.9.2. CAPACIDADE E QUANTIDADES
4.9.2.1. Throughput de, no mínimo, 14.9 Gbps, com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação, anti-malware e prevenção de ameaças avançadas (dia zero) habilitados simultaneamente;
4.9.2.2. Suporte a, no mínimo, 15.900.000 (quinze milhões e novecentas mil) conexões ou sessões simultâneas;
4.9.2.3. Suporte a, no mínimo, 430.000 (quatrocentas e trinta mil) novas conexões ou sessões por segundo;

4.9.2.4. Throughput de, no mínimo, 19 Gbps (dezenove), para conexões VPN;
4.9.2.5. Armazenamento redundante de, no mínimo, 450GB SSD;
4.9.2.6. Possuir, no mínimo, 8 (oito) interfaces de rede 1Gbps UTP;
4.9.2.7. Possuir, no mínimo, 8 (oito) interfaces de rede 10 Gbps SFP+;
4.9.2.8. Suportar expansão para, no mínimo, 2 interfaces de rede 40Gbps QSFP+;
4.9.2.9. Suportar expansão para, no mínimo, 2 interfaces de rede 100/25Gbps QSFP28;
4.9.2.10. Capacidade para suportar até 225 contextos virtuais;
4.9.2.11. Possuir fonte de alimentação redundante e hot-swappable;
4.9.2.12. Possuir 1 (uma) interface de rede dedicada ao gerenciamento;
4.9.2.13. Possuir 1 (uma) interface de rede dedicada para sincronismo;
4.9.2.14. Possuir 1 (uma) interface do tipo console ou similar;
4.9.2.15. 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 fisica/dedicada, deverá ser composta com outro equipamento de terceiro onde faça essa função. Não sendo permitido qualquer tipo de configuração de instancias via software.
4.9.2.16. 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.
4.9.2.17. 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;
4.9.2.18. Todas as interfaces fornecidas nos appliances devem estar licenciadas e habilitadas para uso imediato, incluindo seus transceivers/transceptores. Caso sejam fornecidas interfaces além das exigidas, todas as interfaces devem ser fornecidas com todos os transceivers/transceptores necessários para a plena utilização;

4.9.3. FUNCIONALIDADE DE FIREWALL
4.9.3.1. A solução deve consistir de appliance de proteção de rede com funcionalidades de proteção de próxima geração;
4.9.3.2. 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;
4.9.3.3. 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;
4.9.3.4. Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19”, incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;
4.9.3.5. Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:
4.9.3.6. 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;
4.9.3.7. A solução deve possuir mecanismo onde identifica o volume de conexões que foi trafegada na regra, assim identificando as regras mais utilizadas;
4.9.3.8. Deve suportar os seguintes tipos de NAT:
4.9.3.9. 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;
4.9.3.10. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
4.9.3.11. Deve suportar NAT64 e NAT46;
4.9.3.12. Enviar logs para sistemas de monitoração externos, simultaneamente;
4.9.3.13. 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 aceito soluções que utilizem tabela de roteamento para esta proteção;
4.9.3.14. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);

4.9.3.15. 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);
4.9.3.16. Para IPv6, deve suportar roteamento estático e dinâmico (OSPF);
4.9.3.17. Suportar OSPF graceful restart;
4.9.3.18. Autenticação integrada via Kerberos.
4.9.3.19. Cada regra deve, obrigatoriamente, funcionar nas versões de endereço IP 4 e 6 sem duplicação da base de objetos e regras;
4.9.3.20. Não serão aceitas soluções nas quais as interfaces de origem e destino tenham que ser obrigatoriamente explicitadas ou obrigatoriamente listadas nas configurações de regras;

4.9.4. FUNCIONALIDADE DE CONTROLE DE DADOS E FILTRO DE CONTEÚDO WEB

4.9.4.1. 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;
4.9.4.2. Controle de políticas por usuários, grupos de usuários, IPs e redes;
4.9.4.3. Deve de-criptografar tráfego de entrada e saída em conexões negociadas com TLS 1.2;
4.9.4.4. Será aceito soluções de outros fabricantes diferentes do firewall ofertado pela licitante desde que atendido todos os requisitos desta especificação;
4.9.4.5. Suportar a atribuição de agendamento às políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;
4.9.4.6. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:
4.9.4.7. Deve ser possível a liberação e bloqueio de aplicações sem a necessidade de liberação de portas e protocolos;
4.9.4.8. 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;
4.9.4.9. Para tráfego criptografado (SSL), deve de-criptografar pacotes a fim de possibilitar a leitura do payload para checagem de assinaturas de aplicações conhecidas;
4.9.4.10. A solução deve suportar a recategorização de URLs local;
4.9.4.11. Atualizar a base de assinaturas de aplicações automaticamente;
4.9.4.12. A solução deve permitir a solicitação da contratada com o fabricante para categorização de URL na base do fabricante;
4.9.4.13. Limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD;
4.9.4.14. 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;
4.9.4.15. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos ou análise heurística;
4.9.4.16. 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;
4.9.4.17. A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:
4.9.4.18. Permitir especificar política por tempo, com definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
4.9.4.19. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes;
4.9.4.20. Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;
4.9.4.21. 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;

4.9.4.22. 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;
4.9.4.23. Suportar a criação de categorias de URLs customizadas;
4.9.4.24. Permitir a customização de página de bloqueio;
4.9.4.25. 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;
4.9.4.26. 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;
4.9.4.27. 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);
4.9.4.28. 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:
4.9.4.28.1. PCI – números de cartão de crédito;
4.9.4.28.2. Arquivos PDF;
4.9.4.28.3. Arquivos executáveis;
4.9.4.28.4. Arquivos de banco de dados;
4.9.4.28.5. Arquivos do tipo documento;
4.9.4.28.6. Arquivos do tipo apresentação;
4.9.4.28.7. Arquivos do tipo planilha;
4.9.4.29. 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".
4.9.4.30. 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.
4.9.4.31. 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.

4.9.5. FUNCIONALIDADES DE PREVENÇÃO DE AMEAÇAS

4.9.5.1. 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;
4.9.5.2. Possuir capacidade de detecção de, no mínimo, 7.000 (sete mil) assinaturas de ataques pré-definidos;
4.9.5.3. A solução deve sincronizar ou aplicar as assinaturas de IPS, Antivírus, Anti-Malware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;
4.9.5.4. 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;
4.9.5.5. 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;
4.9.5.6. 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;
4.9.5.7. Detectar e bloquear a origem de portscans;
4.9.5.8. Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações;
4.9.5.9. A solução de IPS, deve suportar a inclusão de novas assinaturas e customização no formato SNORT;
4.9.5.10. Possuir assinaturas para bloqueio de ataques de buffer overflow;

4.9.5.11. Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP;
4.9.5.12. Suportar bloqueio de arquivos por tipo;
4.9.5.13. Identificar e bloquear comunicação com botnets;
4.9.5.14. Deve suportar referência cruzada com CVE;
4.9.5.15. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:
4.9.5.16. O nome da assinatura e do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo de proteção;
4.9.5.17. Deve suportar a captura de pacotes (PCAP), em assinatura de IPS e Anti-Malware, através da console de gerência centralizada;
4.9.5.18. Os eventos devem identificar o país de onde partiu a ameaça;
4.9.5.19. Deve suportar a inspeção em arquivos comprimidos (zip, gzip,etc.);
4.9.5.20. Possuir a capacidade de prevenção de ameaças não conhecidas;
4.9.5.21. Suportar a criação de políticas por Geo Localização, permitindo que o tráfego de determinado País/Países seja bloqueado;
4.9.5.22. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
4.9.5.23. A solução de anti-malware, deve ser capaz de detectar e bloquear ações de callbacks;

4.9.6. FUNCIONALIDADES DE CONTROLE DE QUALIDADE DE SERVIÇO

4.9.6.1. Suportar a criação de políticas de QoS por:
4.9.6.2. Endereço de origem, endereço de destino e por porta;
4.9.6.3. O QoS deve possibilitar a definição de classes por:
4.9.6.3.1. Banda garantida;
4.9.6.3.2. Banda máxima ;
4.9.6.3.3. Fila de prioridade;
4.9.6.4. Disponibilizar estatísticas RealTime para classes de QoS;

4.9.7. FUNCIONALIDADES DE VPN

4.9.7.1. Suportar VPN Site-to-Site e Cliente-To-Site;
4.9.7.2. Suportar IPSec VPN;
4.9.7.3. Suportar SSL VPN;
4.9.7.4. A VPN IPSEc deve suportar:
4.9.7.4.1. 3DES, Autenticação MD5 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;
4.9.7.5. A solução deve suportar CA Interna e CA Externa de terceiros;
4.9.7.6. Solução deve suportar a configuração VPN através de uma interface do tipo GUI (console do fabricante ou interface web);

4.9.8. SOLUÇÃO DE PROTEÇÃO CONTRA AMEAÇAS AVANÇADAS
4.9.8.1. 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;
4.9.8.2. 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.
4.9.8.3. A solução deve ser capaz de inspecionar e prevenir malware desconhecido em tráfego criptografado SSL;
4.9.8.4. 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;
4.9.8.5. 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;

4.9.8.6. A solução deve suportar as seguintes topologias de implantação: Inline, Message Transfer Agent (MTA) e Mirror/TAP;
4.9.8.7. 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;
4.9.8.8. A solução de prevenção de ameaças avançadas (Sandboxing) contra ataques persistentes e Zero-Day, 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.
4.9.8.9. 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 administrador do sistema. As atualizações deverão ser providas pelo fabricante;
4.9.8.10. Para a emulação de arquivos, a solução deve suportar arquivos com tamanho máximo de emulação de até 30Mb.
4.9.8.11. Implementar mecanismo de exceção, permitindo a criação de regras por VLAN, subrede e endereço IP;
4.9.8.12. 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, scr, xls, xlsx, xlt, xlm, xltx, xlsm, xltm, xlsb, xla, xlam, xll, xlw, ppt, pptx, pps, pptm, potx, potm, ppam, ppsx, ppsm, doc, docx, dot, docm, dotx, dotm;
4.9.8.13. A solução deve permitir a criação de Whitelists baseado no MD5 do arquivo;
4.9.8.14. Para melhor administração da solução, a solução deve possibilitar as seguintes visualizações a nível de monitoração:
4.9.8.14.1. Quantidade de arquivos que estão em emulação;
4.9.8.14.2. Número de arquivos emulados;
4.9.8.15. A solução deve possuir os indicadores abaixo referente ao último dia, última semana ou últimos 30 dias:
4.9.8.15.1. Arquivos scaneados;
4.9.8.15.2. Arquivos maliciosos;

4.10. ITEM 10 – NEXT GENERATION FIREWALL – DATA CENTER TIPO III

4.10.1. CARACTERÍSTICAS GERAIS
4.10.1.1. É permitido a composição da solução ofertada entre diversos fabricantes, desde que não contemple solução de software livre;
4.10.1.2. A solução deverá ser compatível com SNMPv2 e SNMPv3;
4.10.1.3. 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;
4.10.1.4. A comunicação entre os appliances de segurança e o módulo de gerência deve ser através de meio criptografado;
4.10.1.5. Os appliances de segurança devem suportar operar em cluster ativo-ativo e ativo-passivo sem a necessidade de licenças adicionais;
4.10.1.6. Não serão aceitos modelos em listas de end-of-sale, cuja data do fim de vendas seja anterior à data da proposta.
4.10.1.7. 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.

4.10.2. CAPACIDADE E QUANTIDADES

4.10.2.1. Throughput de, no mínimo, 23 Gbps, com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação, anti-malware e prevenção de ameaças avançadas (dia zero) habilitados simultaneamente;
4.10.2.2. Suporte a, no mínimo, 19.000.000 (dezenove milhões) conexões ou sessões simultâneas;

4.10.2.3. Suporte a, no mínimo, 540.000 (quinhentos e quarenta mil) novas conexões ou sessões por segundo;
4.10.2.4. Throughput de, no mínimo, 40 Gbps (quarenta), para conexões VPN;
4.10.2.5. Armazenamento redundante de, no mínimo, 200GB SSD ou HDD;
4.10.2.6. Possuir, no mínimo, 8 (oito) interfaces de rede 1Gbps UTP;
4.10.2.7. Possuir, no mínimo, 12 (doze) interfaces de rede 10 Gbps SFP+;
4.10.2.8. Suportar expansão para, no mínimo, 2 interfaces de rede 40Gbps QSFP+;
4.10.2.9. Suportar expansão para, no mínimo, 2 interfaces de rede 100/25Gbps QSFP28;
4.10.2.10. Capacidade para suportar até 225 contextos virtuais;
4.10.2.11. Possuir fonte de alimentação redundante e hot-swappable;
4.10.2.12. Possuir 1 (uma) interface de rede dedicada ao gerenciamento;
4.10.2.13. Possuir 1 (uma) interface de rede dedicada para sincronismo;
4.10.2.14. Possuir 1 (uma) interface do tipo console ou similar;
4.10.2.15. 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 fisica/dedicada, deverá ser composta com outro equipamento de terceiro onde faça essa função. Não sendo permitido qualquer tipo de configuração de instancias via software.
4.10.2.16. 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.
4.10.2.17. 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;
4.10.2.18. Todas as interfaces fornecidas nos appliances devem estar licenciadas e habilitadas para uso imediato, incluindo seus transceivers/transceptores. Caso sejam fornecidas interfaces além das exigidas, todas as interfaces devem ser fornecidas com todos os transceivers/transceptores necessários para a plena utilização;

4.10.3. FUNCIONALIDADE DE FIREWALL
4.10.3.1. A solução deve consistir de appliance de proteção de rede com funcionalidades de proteção de próxima geração;
4.10.3.2. 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;
4.10.3.3. 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;
4.10.3.4. Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19”, incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;
4.10.3.5. Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:
4.10.3.6. 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;
4.10.3.7. A solução deve possuir mecanismo onde identifica o volume de conexões que foi trafegada na regra, assim identificando as regras mais utilizadas;
4.10.3.8. Deve suportar os seguintes tipos de NAT:
4.10.3.9. 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;
4.10.3.10. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
4.10.3.11. Deve suportar NAT64 e NAT46;
4.10.3.12. Enviar logs para sistemas de monitoração externos, simultaneamente;

4.10.3.13. 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;
4.10.3.14. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
4.10.3.15. 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);
4.10.3.16. Para IPv6, deve suportar roteamento estático e dinâmico (OSPF);
4.10.3.17. Suportar OSPF graceful restart;
4.10.3.18. Autenticação integrada via Kerberos.
4.10.3.19. Cada regra deve, obrigatoriamente, funcionar nas versões de endereço IP 4 e 6 sem duplicação da base de objetos e regras;
4.10.3.20. Não serão aceitas soluções nas quais as interfaces de origem e destino tenham que ser obrigatoriamente explicitadas ou obrigatoriamente listadas nas configurações de regras;

4.10.4. FUNCIONALIDADE DE CONTROLE DE DADOS E FILTRO DE CONTEÚDO WEB

4.10.4.1. 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;
4.10.4.2. Controle de políticas por usuários, grupos de usuários, IPs e redes;
4.10.4.3. Deve de-criptografar tráfego de entrada e saída em conexões negociadas com TLS 1.2;
4.10.4.4. Será aceito soluções de outros fabricantes diferentes do firewall ofertado pela licitante desde que atendido todos os requisitos desta especificação;
4.10.4.5. Suportar a atribuição de agendamento às políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;
4.10.4.6. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:
4.10.4.7. Deve ser possível a liberação e bloqueio de aplicações sem a necessidade de liberação de portas e protocolos;
4.10.4.8. 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, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;
4.10.4.9. Para tráfego criptografado (SSL), deve de-criptografar pacotes a fim de possibilitar a leitura do payload para checagem de assinaturas de aplicações conhecidas;
4.10.4.10. A solução deve suportar a recategorização de URLs local;
4.10.4.11. Atualizar a base de assinaturas de aplicações automaticamente;
4.10.4.12. A solução deve permitir a solicitação da contratada com o fabricante para categorização de URL na base do fabricante;
4.10.4.13. Limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD;
4.10.4.14. 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;
4.10.4.15. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos ou análise heurística;
4.10.4.16. 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;
4.10.4.17. A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:
4.10.4.18. Permitir especificar política por tempo, com definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
4.10.4.19. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes;
4.10.4.20. Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;

4.10.4.21. 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;
4.10.4.22. 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;
4.10.4.23. Suportar a criação de categorias de URLs customizadas;
4.10.4.24. Permitir a customização de página de bloqueio;
4.10.4.25. 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;
4.10.4.26. 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;
4.10.4.27. 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);
4.10.4.28. 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:
4.10.4.28.1. PCI – números de cartão de crédito;
4.10.4.28.2. Arquivos PDF;
4.10.4.28.3. Arquivos executáveis;
4.10.4.28.4. Arquivos de banco de dados;
4.10.4.28.5. Arquivos do tipo documento;
4.10.4.28.6. Arquivos do tipo apresentação;
4.10.4.28.7. Arquivos do tipo planilha;
4.10.4.29. 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".
4.10.4.30. 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.
4.10.4.31. 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.

4.10.5. FUNCIONALIDADES DE PREVENÇÃO DE AMEAÇAS

4.10.5.1. 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;
4.10.5.2. Possuir capacidade de detecção de, no mínimo, 7.000 (sete mil) assinaturas de ataques pré-definidos;
4.10.5.3. A solução deve sincronizar ou aplicar as assinaturas de IPS, Antivírus, Anti-Malware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;
4.10.5.4. 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;
4.10.5.5. 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;
4.10.5.6. 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;
4.10.5.7. Detectar e bloquear a origem de portscans;
4.10.5.8. Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações;

4.10.5.9. A solução de IPS, deve suportar a inclusão de novas assinaturas e customização no formato SNORT;
4.10.5.10. Possuir assinaturas para bloqueio de ataques de buffer overflow;
4.10.5.11. Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP;
4.10.5.12. Suportar bloqueio de arquivos por tipo;
4.10.5.13. Identificar e bloquear comunicação com botnets;
4.10.5.14. Deve suportar referência cruzada com CVE;
4.10.5.15. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:
4.10.5.16. O nome da assinatura e do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo de proteção;
4.10.5.17. Deve suportar a captura de pacotes (PCAP), em assinatura de IPS e Anti-Malware, através da console de gerência centralizada;
4.10.5.18. Os eventos devem identificar o país de onde partiu a ameaça;
4.10.5.19. Deve suportar a inspeção em arquivos comprimidos (zip, gzip,etc.);
4.10.5.20. Possuir a capacidade de prevenção de ameaças não conhecidas;
4.10.5.21. Suportar a criação de políticas por Geo Localização, permitindo que o tráfego de determinado País/ Países seja bloqueado;
4.10.5.22. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
4.10.5.23. A solução de anti-malware, deve ser capaz de detectar e bloquear ações de callbacks;

4.10.6. FUNCIONALIDADES DE CONTROLE DE QUALIDADE DE SERVIÇO

4.10.6.1. Suportar a criação de políticas de QoS por:
4.10.6.2. Endereço de origem, endereço de destino e por porta;
4.10.6.3. O QoS deve possibilitar a definição de classes por:
4.10.6.3.1. Banda garantida;
4.10.6.3.2. Banda máxima ;
4.10.6.3.3. Fila de prioridade;
4.10.6.4. Disponibilizar estatísticas RealTime para classes de QoS;

4.10.7. FUNCIONALIDADES DE VPN

4.10.7.1. Suportar VPN Site-to-Site e Cliente-To-Site;
4.10.7.2. Suportar IPSec VPN;
4.10.7.3. Suportar SSL VPN;
4.10.7.4. A VPN IPSEc deve suportar:
4.10.7.4.1. 3DES, Autenticação MD5 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;
4.10.7.5. A solução deve suportar CA Interna e CA Externa de terceiros;
4.10.7.6. Solução deve suportar a configuração VPN através de uma interface do tipo GUI (console do fabricante ou interface web);

4.10.8. SOLUÇÃO DE PROTEÇÃO CONTRA AMEAÇAS AVANÇADAS

4.10.8.1. 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 da próprio fabricante ou appliance dedicada para sandboxing;
4.10.8.2. 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.
4.10.8.3. A solução deve ser capaz de inspecionar e prevenir malware desconhecido em tráfego criptografado SSL;

4.10.8.4. 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 2016;
4.10.8.5. 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;
4.10.8.6. A solução deve suportar as seguintes topologias de implantação: Inline, Message Transfer Agent (MTA) e Mirror/TAP;
4.10.8.7. 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;
4.10.8.8. A solução de prevença de ameaças avançadas (Sandboxing) contra ataques persistentes e Zero-Day, 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.
4.10.8.9. 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;
4.10.8.10. Para a emulação de arquivos, a solução deve suportar arquivos com tamanho máximo de emulação de até 30Mb.
4.10.8.11. Implementar mecanismo de exceção, permitindo a criação de regras por VLAN, subrede e endereço IP;
4.10.8.12. 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, scr, xls, xlsx, xlt, xlm, xltx, xlsm, xltm, xlsb, xla, xlam, xll, xlw, ppt, pptx, pps, pptm, potx, potm, ppam, ppsx, ppsm, doc, docx, dot, docm, dotx, dotm;
4.10.8.13. A solução deve permitir a criação de Whitelists baseado no MD5 do arquivo;
4.10.8.14. Para melhor administração da solução, a solução deve possibilitar as seguintes visualizações a nível de monitoração:
4.10.8.14.1. Quantidade de arquivos que estão em emulação;
4.10.8.14.2. Número de arquivos emulados;
4.10.8.15. A solução deve possuir os indicadores abaixo referente ao último dia, última semana ou últimos 30 dias:
4.10.8.15.1. Arquivos scaneados;
4.10.8.15.2. Arquivos maliciosos;

4.11. ITEM 11 – NEXT GENERATION FIREWALL PARA NUVEM PRIVADA

4.11.1. CARACTERÍSTICAS GERAIS
4.11.1.1. O licenciamento deverá ser feito pelo número de cores virtuais;
4.11.1.2. Deve ser compatível com, pelo menos, os seguintes hypervisors: VMware ESXi, Microsoft Hyper-V e KVM;
4.11.1.3. A solução deverá permitir expansão através de adição de novas licenças, de forma que suporte a criação de "pools" de gateways virtuais;
4.11.1.4. A solução para ambientes virtualizados deve suportar os seguintes SDN de mercado para integração, como: OpenStack, Cisco ACI, VMware NSX, e ESXi.

4.11.2. FUNCIONALIDADE DE FIREWALL
4.11.2.1. A solução deve consistir de appliance de proteção de rede com funcionalidades de proteção de próxima geração;
4.11.2.2. 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;
4.11.2.3. Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:
4.11.2.4. 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;

4.11.2.5. A solução deve possuir mecanismo onde identifica o volume de conexões que foi trafegada na regra, assim identificando as regras mais utilizadas;
4.11.2.6. Deve suportar os seguintes tipos de NAT:
4.11.2.6.1. 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;
4.11.2.7. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
4.11.2.8. Deve suportar NAT64 e NAT46;
4.11.2.9. Enviar logs para sistemas de monitoração externos, simultaneamente;
4.11.2.10. 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;
4.11.2.11. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
4.11.2.12. 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);
4.11.2.13. Para IPv6, deve suportar roteamento estático e dinâmico (OSPF);
4.11.2.14. Suportar OSPF graceful restart;
4.11.2.15. Autenticação integrada via Kerberos.
4.11.2.16. Cada regra deve, obrigatoriamente, funcionar nas versões de endereço IP 4 e 6 sem duplicação da base de objetos e regras;
4.11.2.17. Não serão aceitas soluções nas quais as interfaces de origem e destino tenham que ser obrigatoriamente explicitadas ou obrigatoriamente listadas nas configurações de regras;

4.11.3. FUNCIONALIDADE DE CONTROLE DE DADOS E FILTRO DE CONTEÚDO WEB

4.11.3.1. 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;
4.11.3.2. Controle de políticas por usuários, grupos de usuários, IPs e redes;
4.11.3.3. Deve de-criptografar tráfego de entrada e saída em conexões negociadas com TLS 1.2;
4.11.3.4. Será aceito soluções de outros fabricantes diferentes do firewall ofertado pela licitante desde que atendido todos os requisitos desta especificação;
4.11.3.5. Suportar a atribuição de agendamento às políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;
4.11.3.6. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:
4.11.3.7. Deve ser possível a liberação e bloqueio de aplicações sem a necessidade de liberação de portas e protocolos;
4.11.3.8. 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;
4.11.3.9. Para tráfego criptografado (SSL), deve de-criptografar pacotes a fim de possibilitar a leitura do payload para checagem de assinaturas de aplicações conhecidas;
4.11.3.10. A solução deve suportar a recategorização de URLs local;
4.11.3.11. Atualizar a base de assinaturas de aplicações automaticamente;
4.11.3.12. A solução deve permitir a solicitação da contratada com o fabricante para categorização de URL na base do fabricante;
4.11.3.13. Limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD;
4.11.3.14. 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;

4.11.3.15. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos ou análise heurística;
4.11.3.16. 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;
4.11.3.17. A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:
4.11.3.18. Permitir especificar política por tempo, com definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
4.11.3.19. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes;
4.11.3.20. Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;
4.11.3.21. 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;
4.11.3.22. 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;
4.11.3.23. Suportar a criação de categorias de URLs customizadas;
4.11.3.24. Permitir a customização de página de bloqueio;
4.11.3.25. 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;
4.11.3.26. 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;
4.11.3.27. 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);
4.11.3.28. 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:
4.11.3.28.1. PCI – números de cartão de crédito;
4.11.3.28.2. Arquivos PDF;
4.11.3.28.3. Arquivos executáveis;
4.11.3.28.4. Arquivos de banco de dados;
4.11.3.28.5. Arquivos do tipo documento;
4.11.3.28.6. Arquivos do tipo apresentação;
4.11.3.28.7. Arquivos do tipo planilha;
4.11.3.29. 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".
4.11.3.30. 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.
4.11.3.31. 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.

4.11.4. FUNCIONALIDADES DE PREVENÇÃO DE AMEAÇAS

4.11.4.1. 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;
4.11.4.2. Possuir capacidade de detecção de, no mínimo, 7.000 (sete mil) assinaturas de ataques pré-definidos;
4.11.4.3. A solução deve sincronizar ou aplicar as assinaturas de IPS, Antivírus, Anti-Malware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;
4.11.4.4. 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;

4.11.4.5. 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;
4.11.4.6. 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;
4.11.4.7. Detectar e bloquear a origem de portscans;
4.11.4.8. Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações;
4.11.4.9. A solução de IPS, deve suportar a inclusão de novas assinaturas e customização no formato SNORT;
4.11.4.10. Possuir assinaturas para bloqueio de ataques de buffer overflow;
4.11.4.11. Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP;
4.11.4.12. Suportar bloqueio de arquivos por tipo;
4.11.4.13. Identificar e bloquear comunicação com botnets;
4.11.4.14. Deve suportar referência cruzada com CVE;
4.11.4.15. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:
4.11.4.16. O nome da assinatura e do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo de proteção;
4.11.4.17. Deve suportar a captura de pacotes (PCAP), em assinatura de IPS e Anti-Malware, através da console de gerência centralizada;
4.11.4.18. Os eventos devem identificar o país de onde partiu a ameaça;
4.11.4.19. Deve suportar a inspeção em arquivos comprimidos (zip, gzip,etc.);
4.11.4.20. Possuir a capacidade de prevenção de ameaças não conhecidas;
4.11.4.21. Suportar a criação de políticas por Geo Localização, permitindo que o tráfego de determinado País/Países seja bloqueado;
4.11.4.22. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
4.11.4.23. A solução de anti-malware, deve ser capaz de detectar e bloquear ações de callbacks;

4.11.5. FUNCIONALIDADES DE CONTROLE DE QUALIDADE DE SERVIÇO

4.11.5.1. Suportar a criação de políticas de QoS por:
4.11.5.2. Endereço de origem, endereço de destino e por porta;
4.11.5.3. O QoS deve possibilitar a definição de classes por:
4.11.5.3.1. Banda garantida;
4.11.5.3.2. Banda máxima ;
4.11.5.3.3. Fila de prioridade;
4.11.5.4. Disponibilizar estatísticas RealTime para classes de QoS;

4.11.6. FUNCIONALIDADES DE VPN

4.11.6.1. Suportar VPN Site-to-Site e Cliente-To-Site;
4.11.6.2. Suportar IPSec VPN;
4.11.6.3. Suportar SSL VPN;
4.11.6.4. A VPN IPSEc deve suportar:
4.11.6.4.1. 3DES, Autenticação MD5 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;
4.11.6.5. A solução deve suportar CA Interna e CA Externa de terceiros;
4.11.6.6. Solução deve suportar a configuração VPN através de uma interface do tipo GUI (console do fabricante ou interface web);

4.11.7. SOLUÇÃO DE PROTEÇÃO CONTRA AMEAÇAS AVANÇADAS

4.11.7.1. 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 da próprio fabricante ou appliance dedicada para sandboxing;
4.11.7.2. 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 sandbox, sem que o mesmo seja entregue parcialmente ao cliente.
4.11.7.3. A solução deve ser capaz de inspecionar e prevenir malware desconhecido em tráfego criptografado SSL;
4.11.7.4. 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 2016;
4.11.7.5. 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;
4.11.7.6. A solução deve suportar as seguintes topologias de implantação: Inline, Message Transfer Agent (MTA) e Mirror/TAP;
4.11.7.7. 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;
4.11.7.8. A solução de prevença de ameaças avançadas (Sandboxing) contra ataques persistentes e Zero-Day, 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.
4.11.7.9. 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;
4.11.7.10. Para a emulação de arquivos, a solução deve suportar arquivos com tamanho máximo de emulação de até 30Mb.
4.11.7.11. Implementar mecanismo de exceção, permitindo a criação de regras por VLAN, subrede e endereço IP;
4.11.7.12. 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, scr, xls, xlsx, xlt, xlm, xltx, xlsm, xltm, xlsb, xla, xlam, xll, xlw, ppt, pptx, pps, pptm, potx, potm, ppam, ppsx, ppsm, doc, docx, dot, docm, dotx, dotm;
4.11.7.13. A solução deve permitir a criação de Whitelists baseado no MD5 do arquivo;
4.11.7.14. Para melhor administração da solução, a solução deve possibilitar as seguintes visualizações a nível de monitoração:
4.11.7.14.1. Quantidade de arquivos que estão em emulação;
4.11.7.14.2. Número de arquivos emulados;
4.11.7.15. A solução deve possuir os indicadores abaixo referente ao último dia, última semana ou últimos 30 dias:
4.11.7.15.1. Arquivos scaneados;
4.11.7.15.2. Arquivos maliciosos;

4.12. ITEM 12 – NEXT GENERATION FIREWALL PARA NUVEM PÚBLICA

4.12.1. CARACTERÍSTICAS GERAIS
4.12.1.1. A solução deve estar listada como parceiro de segurança, pelo menos, da AWS, Azure e Google Cloud Platform (GCP) e Oracle Cloud (OCI).
4.12.1.2. A solução dever fazer parte do market place, pelo menos, da AWS e Azure.
4.12.1.3. A solução deve possuir, pelo menos, os métodos de licenciamento “pay as you go” e “bring your own license”
4.12.1.4. A solução deve suportar políticas de segurança dinâmicas que utilizem os objetos definidos na AWS ajustando automaticamente a segurança com as mudanças que ocorrem num ambiente dinâmico de nuvem.
4.12.1.5. Deve ser capaz de utilizar objetos, pelo menos, da AWS e da Azure nas políticas de segurança;

4.12.1.6. Deve ser capaz de receber atualizações automáticas de objetos localizados, pelo menos, na AWS e na Azure, sem a necessidade de alterar a política;

4.12.2. FUNCIONALIDADE DE FIREWALL

4.12.2.1. A solução deve consistir de appliance de proteção de rede com funcionalidades de proteção de próxima geração;

4.12.2.2. 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;

4.12.2.3. Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:

4.12.2.4. 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;

4.12.2.5. A solução deve possuir mecanismo onde identifica o volume de conexões que foi trafegada na regra, assim identificando as regras mais utilizadas;

4.12.2.6. Deve suportar os seguintes tipos de NAT:

4.12.2.7. 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;

4.12.2.8. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;

4.12.2.9. Deve suportar NAT64 e NAT46;

4.12.2.10. Enviar logs para sistemas de monitoração externos, simultaneamente;

4.12.2.11. 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;

4.12.2.12. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);

4.12.2.13. 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);

4.12.2.14. Para IPv6, deve suportar roteamento estático e dinâmico (OSPF);

4.12.2.15. Suportar OSPF graceful restart;

4.12.2.16. Autenticação integrada via Kerberos.

4.12.2.17. Cada regra deve, obrigatoriamente, funcionar nas versões de endereço IP 4 e 6 sem duplicação da base de objetos e regras;

4.12.2.18. Não serão aceitas soluções nas quais as interfaces de origem e destino tenham que ser obrigatoriamente explicitadas ou obrigatoriamente listadas nas configurações de regras;

4.12.3. FUNCIONALIDADE DE CONTROLE DE DADOS E FILTRO DE CONTEÚDO WEB

4.12.3.1. 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;

4.12.3.2. Controle de políticas por usuários, grupos de usuários, IPs e redes;

4.12.3.3. Deve de-criptografar tráfego de entrada e saída em conexões negociadas com TLS 1.2;

4.12.3.4. Será aceito soluções de outros fabricantes diferentes do firewall ofertado pela licitante desde que atendido todos os requisitos desta especificação;

4.12.3.5. Suportar a atribuição de agendamento às políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

4.12.3.6. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:

4.12.3.7. Deve ser possível a liberação e bloqueio de aplicações sem a necessidade de liberação de portas e protocolos;

4.12.3.8. 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;

4.12.3.9. Para tráfego criptografado (SSL), deve de-criptografar pacotes a fim de possibilitar a leitura do payload para checagem de assinaturas de aplicações conhecidas;
4.12.3.10. A solução deve suportar a recategorização de URLs local;
4.12.3.11. Atualizar a base de assinaturas de aplicações automaticamente;
4.12.3.12. A solução deve permitir a solicitação da contratada com o fabricante para categorização de URL na base do fabricante;
4.12.3.13. Limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD;
4.12.3.14. 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;
4.12.3.15. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos ou análise heurística;
4.12.3.16. 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;
4.12.3.17. A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:
4.12.3.18. Permitir especificar política por tempo, com definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
4.12.3.19. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes;
4.12.3.20. Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;
4.12.3.21. 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;
4.12.3.22. 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;
4.12.3.23. Suportar a criação de categorias de URLs customizadas;
4.12.3.24. Permitir a customização de página de bloqueio;
4.12.3.25. 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;
4.12.3.26. 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;
4.12.3.27. 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);
4.12.3.28. 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:
4.12.3.28.1. PCI – números de cartão de crédito;
4.12.3.28.2. Arquivos PDF;
4.12.3.28.3. Arquivos executáveis;
4.12.3.28.4. Arquivos de banco de dados;
4.12.3.28.5. Arquivos do tipo documento;
4.12.3.28.6. Arquivos do tipo apresentação;
4.12.3.28.7. Arquivos do tipo planilha;
4.12.3.29. 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".
4.12.3.30. 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.
4.12.3.31. 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.

4.12.4. FUNCIONALIDADES DE PREVENÇÃO DE AMEAÇAS

4.12.4.1. 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;
4.12.4.2. Possuir capacidade de detecção de, no mínimo, 7.000 (sete mil) assinaturas de ataques pré-definidos;
4.12.4.3. A solução deve sincronizar ou aplicar as assinaturas de IPS, Antivírus, Anti-Malware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;
4.12.4.4. 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;
4.12.4.5. 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;
4.12.4.6. 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;
4.12.4.7. Detectar e bloquear a origem de portscans;
4.12.4.8. Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações;
4.12.4.9. A solução de IPS, deve suportar a inclusão de novas assinaturas e customização no formato SNORT;
4.12.4.10. Possuir assinaturas para bloqueio de ataques de buffer overflow;
4.12.4.11. Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP;
4.12.4.12. Suportar bloqueio de arquivos por tipo;
4.12.4.13. Identificar e bloquear comunicação com botnets;
4.12.4.14. Deve suportar referência cruzada com CVE;
4.12.4.15. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:
4.12.4.16. O nome da assinatura e do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo de proteção;
4.12.4.17. Deve suportar a captura de pacotes (PCAP), em assinatura de IPS e Anti-Malware, através da console de gerência centralizada;
4.12.4.18. Os eventos devem identificar o país de onde partiu a ameaça;
4.12.4.19. Deve suportar a inspeção em arquivos comprimidos (zip, gzip,etc.);
4.12.4.20. Possuir a capacidade de prevenção de ameaças não conhecidas;
4.12.4.21. Suportar a criação de políticas por Geo Localização, permitindo que o tráfego de determinado País/Países seja bloqueado;
4.12.4.22. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
4.12.4.23. A solução de anti-malware, deve ser capaz de detectar e bloquear ações de callbacks;

4.12.5. FUNCIONALIDADES DE CONTROLE DE QUALIDADE DE SERVIÇO

4.12.5.1. Suportar a criação de políticas de QoS por:
4.12.5.2. Endereço de origem, endereço de destino e por porta;
4.12.5.3. O QoS deve possibilitar a definição de classes por:
4.12.5.4. Banda garantida;
4.12.5.5. Banda máxima ;
4.12.5.6. Fila de prioridade;
4.12.5.7. Disponibilizar estatísticas RealTime para classes de QoS;

4.12.6. FUNCIONALIDADES DE VPN

4.12.6.1. Suportar VPN Site-to-Site e Cliente-To-Site;
4.12.6.2. Suportar IPSec VPN;

4.12.6.3. Suportar SSL VPN;
4.12.6.4. A VPN IPSEc deve suportar:
4.12.6.4.1. 3DES, Autenticação MD5 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;
4.12.6.5. A solução deve suportar CA Interna e CA Externa de terceiros;
4.12.6.6. Solução deve suportar a configuração VPN através de uma interface do tipo GUI (console do fabricante ou interface web);

4.12.7. SOLUÇÃO DE PROTEÇÃO CONTRA AMEAÇAS AVANÇADAS

4.12.7.1. 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 da próprio fabricante ou appliance dedicada para sandboxing;
4.12.7.2. 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 sandbox, sem que o mesmo seja entregue parcialmente ao cliente.
4.12.7.3. A solução deve ser capaz de inspecionar e prevenir malware desconhecido em tráfego criptografado SSL;
4.12.7.4. 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 2016;
4.12.7.5. 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;
4.12.7.6. A solução deve suportar as seguintes topologias de implantação: Inline, Message Transfer Agent (MTA) e Mirror/TAP;
4.12.7.7. 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;
4.12.7.8. A solução de prevença de ameaças avançadas (Sandboxing) contra ataques persistentes e Zero-Day, 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.
4.12.7.9. 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;
4.12.7.10. Para a emulação de arquivos, a solução deve suportar arquivos com tamanho máximo de emulação de até 30Mb.
4.12.7.11. Implementar mecanismo de exceção, permitindo a criação de regras por VLAN, subrede e endereço IP;
4.12.7.12. 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, scr, xls, xlsx, xlt, xlm, xltx, xlsm, xltm, xlsb, xla, xlam, xll, xlw, ppt, pptx, pps, pptm, potx, potm, ppam, ppsx, ppsm, doc, docx, dot, docm, dotx, dotm;
4.12.7.13. A solução deve permitir a criação de Whitelists baseado no MD5 do arquivo;
4.12.7.14. Para melhor administração da solução, a solução deve possibilitar as seguintes visualizações a nível de monitoração:
4.12.7.14.1. Quantidade de arquivos que estão em emulação;
4.12.7.15. Número de arquivos emulados;
4.12.7.16. A solução deve possuir os indicadores abaixo referente ao último dia, última semana ou últimos 30 dias:
4.12.7.16.1. Arquivos scaneados;
4.12.7.16.2. Arquivos maliciosos;

4.13. ITEM 13 – SOLUÇÃO DE GERÊNCIA DE POSTURA DE SEGURANÇA PARA NUVENS PÚBLICAS

4.13.1.1. Deve suportar ambientes multi-cloud, incluindo Azure, AWS e Google.

4.13.1.2. A solução deverá ser capaz de montar uma topologia em tempo real dos grupos de segurança e suas relações entre as políticas de segurança.

4.13.1.3. A solução deverá ser capaz de visualizar o fluxo de tráfego e os tráfegos dropados entre os assets, grupos de segurança e instâncias.

4.13.1.4. A solução deverá ser capaz de visualização de modelos de arquitetura para inspecionar e colaborar antes de uma implantação (ex: AWS CloudFormation ou CFTs).

4.13.1.5. A solução deverá realizar coleta automatizada de informações dos ambientes AWS, Azure e Google Cloud, sem a necessidade de agentes e classificar de forma automática os assets protegidos com base no nível de exposição ao mundo exterior (internet).

4.13.1.6. A solução deverá monitorar o tráfego da rede de carga de trabalho de nuvem de ingresso e saída em tempo real e histórico e correlacione com outros conjuntos de dados para interpretar o contexto.

4.13.1.7. Deve identificar o tráfego proveniente da Internet em portas privilegiadas (ftp, ssh, web, rdp) para serviços que não são tipicamente voltadas para a Internet (bancos de dados, serviços de autenticação, sistemas de gerenciamento de contêineres, etc.)

4.13.1.8. Deverá acionar ações automatizadas para responder a ameaças específicas, incluindo verificação de vulnerabilidades, isolamento de host/workload e remoção de ameaças.

4.13.1.9. Deve ser capaz de realizar investigações sobre dados históricos para garantir que possíveis incidentes de rede possam ser rastreados até sua origem.

4.13.1.10. Deve ser possível realizar investigação de incidente, usando um mapa de risco interativo.

4.13.1.11. A solução deverá detectar eventos de ameaças à rede a partir de feeds de provedores de serviços de nuvem (por exemplo, Amazon GuardDuty, Central de Segurança do Azure, AWS CloudWatch, AWS CloudTrail e Logs de Atividades do Azure).

4.13.1.12. A solução deve permitir login via SSO usando o provedor de identidade personalizado com SAML ou oAUTH2.

4.13.1.13. Deve ser capaz de executar combinações de informações de monitoramento, avaliação e conformidade e fornecer um meio para identificar e priorizar riscos com a assinatura da nuvem.

4.13.1.14. A solução deverá detectar o comprometimento da conta e as ameaças internas, estabelecendo baselines e alertando sobre desvios de baselines.

4.13.1.15. Deverá correlacionar conjuntos de dados para identificar recursos (nome/tag, conta, região etc.)

4.13.1.16. Deverá correlacionar conjuntos de dados para identificar aplicativos

4.13.1.17. Deverá correlacionar conjuntos de dados para criar mapeamento de fluxo

4.13.1.18. Deverá fornecer interface visual intuitiva para investigar o tráfego de rede, incluindo o contexto completo em torno de cargas de trabalho (identificar funções, tags associadas, regras de firewall, etc.), e comportamento do tráfego.

4.13.1.19. Deverá monitorar as configurações de função do IAM e a capacidade de corrigir automaticamente possíveis problemas

4.13.1.20. Deve ser capaz de integrar com estruturas de conformidade, como CIS Benchmark, GDPR, PCI-DSS, NIST, FFIEC, PCI Hi-Trust, ISO, etc.

4.13.1.21. Deve ter capacidade de manter-se atualizado com as mudanças nas estruturas de conformidade e suporte para novas versões.

4.13.1.22. Deve ter capacidade de monitorar e relatar discrepâncias entre os padrões de estrutura e as configurações de recursos implantados na nuvem.

4.13.1.23. Deve ser capaz de atualizar as regras de conformidade com campos personalizado.

4.14. ITEM 14 - SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO E RELATÓRIOS PARA ATÉ 5 EQUIPAMENTOS

4.14.1. Gerência centralizada e relatoria para até 5 equipamentos, compatível com os firewalls dos itens 1 à 10 deste TR.

4.14.2. A solução de gerência centralizada e relatoria ofertada deve atender aos requisitos técnicos descritos no ANEXO A deste TR.

4.15. ITEM 15 - SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO E RELATÓRIOS PARA ATÉ 10 EQUIPAMENTOS

4.15.1. Gerência centralizada e relatoria para até 10 equipamentos, compatível com os firewalls dos itens 1 à 10 deste TR.
4.15.2. A solução de gerência centralizada e relatoria ofertada deve atender aos requisitos técnicos descritos no ANEXO A deste TR.

4.16. ITEM 16 - SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO E RELATÓRIOS PARA ATÉ 50 EQUIPAMENTOS

4.16.1. Gerência centralizada e relatoria para até 50 equipamentos, compatível com os firewalls dos itens 1 à 10 deste TR.
4.16.2. A solução de gerência centralizada e relatoria ofertada deve atender aos requisitos técnicos descritos no ANEXO A deste TR.

4.17. ITEM 17 - SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO E RELATÓRIOS PARA ATÉ 150 EQUIPAMENTOS

4.17.1. Gerência centralizada e relatoria para até 150 equipamentos, compatível com os firewalls dos itens 1 à 10 deste TR.
4.17.2. A solução de gerência centralizada e relatoria ofertada deve atender aos requisitos técnicos descritos no ANEXO A deste TR.

4.18. ITEM 18 - SOLUÇÃO DE NEXT GENERATION ANTI-MALWARE E ANTI-RANSOMWARE COM GERÊNCIA EM NUVEM

4.18.1. CARACTERÍSTICAS GERAIS
4.18.1.1. É permitida a composição da solução ofertada entre diversos fabricantes, desde que não contemple solução de software livre;
4.18.1.2. 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.
4.18.1.3. A solução deverá ser gerenciada centralmente através de portal em nuvem fornecido pelo fabricante da solução ou em nuvem privada fornecida pela licitante;
4.18.1.4. O acesso ao portal de gerenciamento em nuvem deverá ser seguro, através de HTTPS;
4.18.1.5. Deve escanear arquivos e identificar infecções baseado em características comportamentais dos vírus;
4.18.1.6. Deve escanear arquivos quando eles forem acessados, executados, permitindo detecção imediata e tratamento por qualquer ameaça;
4.18.1.7. Deve permitir executar uma análise detalhada de cada arquivo conforme selecionado pelo usuário;
4.18.1.8. Deve permitir especificar diretórios e extensões de arquivos para que sejam excluídos da análise de vírus;
4.18.1.9. Deve checar as áreas mais comuns do sistema de arquivos e a registry do sistema operacional em busca de ameaças avançadas;
4.18.1.10. Deve possuir as seguintes opções de remediação:
4.18.1.10.1. Reparar;
4.18.1.10.2. Quarentenar;

4.18.1.10.3. Apagar;
4.18.1.11. Deve permitir ser gerenciado através de console unificada para gerenciamento centralizado de políticas e logs.
4.18.1.12. Deve identificar automaticamente o ponto de entrada do malware e o seu impacto para a organização;
4.18.1.13. A solução deve suportar os sistemas operacionais:
4.18.1.13.1. Windows 7 (32 e 64 bits);
4.18.1.13.2. Windows 8.1 (32 e 64 bits);
4.18.1.13.3. Windows 10 (32 e 64 bits);
4.18.1.13.4. Windows Server 2008 R2 (32 e 64 bits);
4.18.1.13.5. Windows Server 2012 R2 (64 bits);
4.18.1.13.6. Windows Server 2012 (64 bits);
4.18.1.13.7. Windows Server 2016 (64 bits);
4.18.1.13.8. Windows Server 2019 (64 bits);
4.18.1.14. Deve gerar automaticamente relatório completo da execução do malware utilizando técnicas contidas no MITRE Framework;
4.18.1.15. Deve bloquear ataques independentemente se o vetor de distribuição é baseado na web, e-mail ou mídia removível;
4.18.1.16. 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;
4.18.1.17. 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;
4.18.1.18. 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.
4.18.1.19. O malware detectado deve ser impedido de baixar (a sessão de download é interceptada pelo endpoint). Se o malware já estiver na máquina, ele será colocado em quarentena.
4.18.1.20. 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.
4.18.1.21. Além das ferramentas de solução de problemas padrão, as informações de forense podem ajudar na identificação de tais interferências;
4.18.1.22. 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;
4.18.1.23. 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;
4.18.1.24. 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;
4.18.1.25. Deve possuir análise de campos de login e senha em caso de acesso a páginas internet como e-mail e formulários na detecção e prevenção de sites de phishing;
4.18.1.26. Deve possuir proteção contra reuso de credenciais;
4.18.1.27. A solução deverá detectar e bloquear em tempo real qualquer tipo de ataque de dia zero;
4.18.1.28. A solução deve ser capaz de fazer remediação de forma automatizada, sem a necessidade da intervenção do usuário;
4.18.1.29. 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.
4.18.1.30. 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.
4.18.1.31. 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.

4.18.1.32. 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;
4.18.1.33. Deve reverter as ações do ransomware, restaurando os dados corporativos automaticamente, garantindo proteção contra criptografia dos dados;
4.18.1.34. Possuir tecnologia que não seja baseada apenas em assinaturas, garantindo seu funcionamento tanto de forma online quanto offline;
4.18.1.35. Deve permitir que os usuários obtenham políticas e atualizações de uma pasta compartilhada, sem uma conexão com um serviço e gerenciamento.
4.18.1.36. Deve implementar, através de análise dinâmica e heurística, proteção em tempo real contra sites conhecidos e desconhecidos de phishing;
4.18.1.37. Deve detectar, através de análise estática e heurística, elementos suspeitos em sites que solicitem credenciais dos usuários;
4.18.1.38. Deve detectar e prevenir a reutilização de credenciais corporativas em sites externos;
4.18.1.39. Deve suportar o monitoramento do Log de Eventos do Windows para analisar eventos de malware de fornecedores de antivírus de terceiros.
4.18.1.40. Deve ser capaz de realizar ações com base no Log de Eventos do Windows, como:
4.18.1.40.1. Analisar ataques,
4.18.1.40.2. Encerrar processos,
4.18.1.40.3. Excluir ou colocar arquivos em quarentena
4.18.1.41. Deve possuir processo de análise forense automático de incidentes, disponibilizando as seguintes informações sobre o ataque:
4.18.1.41.1. Eventos Maliciosos;
4.18.1.41.2. Ponto de entrada do malware;
4.18.1.41.3. Escopo dos danos causados;
4.18.1.41.4. Máquinas infectadas;
4.18.2. Gerenciamento Centralizado de políticas de Segurança, Logs e relatórios:
4.18.2.1. A gerência dos endpoints deve ser realizada através de console própria ou através de interface web (HTTPS).
4.18.2.2. Deve ser capaz de gerenciar todos os endpoint de forma centralizada, possibilitando a concentração dos logs e emissão de relatórios.
4.18.2.3. Permitir a criação e distribuição de políticas de segurança de forma centralizada, suportando organização hierárquica de regras em todos os equipamentos.
4.18.2.4. 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.
4.18.2.5. Acesso avançado para monitorar e gerenciar as funções do sistema
4.18.2.6. A solução deve ter integração com o Microsoft Active Directory para identificação de usuários
4.18.2.7. A solução deve incluir a opção de pesquisar dentro da lista de eventos, drill-down em detalhes para a investigação e análise dos eventos;
4.18.2.8. A solução deve apresentar sumario apontando os agentes que estão instalados, em progresso ou que ainda estão pendentes;
4.18.2.9. A gerência deve apontar os agentes nos endpoints que foram violados com Segurança;
4.18.2.10. Todos os logs deverão ser referenciados com o nome do usuário devido a integração com o Active Directory.
4.18.2.11. A solução deve possuir outras funcionalidades de Segurança onde podem ser incorporadas na mesma gerencia.
4.18.2.12. Disponibilizar informações gráficas, na linha tempo que informe o número de eventos ocorridos
4.18.2.13. Disponibilizar recursos interativos de navegação nos eventos informados;
4.18.2.14. A solução deve possuir relatórios customizáveis onde seja possível pegar diferentes informações para montagem do relatório;
4.18.2.15. Correlacionar eventos capaz de utilizar como base informações o número de conexões em determinado tempo seguido pelo menos das ações:

4.18.2.15.1. Bloqueio da origem;
4.18.2.15.2. Envio de SNMP;
4.18.2.15.3. Envio de e-mail;
4.18.2.16. A solução deve exportar relatórios em pelo menos um dos formatos: HTML, CSV e MHT;
4.18.2.17. A solução deve possibilitar a visualização geográfica dos eventos de segurança correlacionados;
4.18.2.18. 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.
4.18.2.19. A solução deve prover no mínimo as seguintes funcionalidades para análise avançada dos incidentes:
4.18.2.20. Gráficos com principais eventos de segurança de acordo com a funcionalidade selecionada;
4.18.2.21. Estatísticas com comparativo de período (hora, dia e mês);
4.18.2.22. 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;
4.18.2.23. A solução deve incluir a opção de pesquisar dentro da lista de eventos, drill-down em detalhes para a investigação e análise dos eventos;
4.18.2.24. 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.
4.18.2.25. Solução deve ser capaz de detectar ataques de tentativa de login e senha utilizando tipos diferentes de credencias;
4.18.2.26. Deve estar inclusa na lista de eventos a opção de gerar automaticamente gráficos ou tabelas com o evento, a origem e distribuição de destino.
4.18.2.27. Deve detectar ataques de negação de serviço e correlacionar eventos de todas as fontes.
4.18.2.28. Deve estar incluso no dashboard com horários predefinidos, diários, semanais e relatórios mensais. Incluindo:
4.18.2.28.1. Top eventos,
4.18.2.28.2. Top origem,
4.18.2.28.3. Top destinos,
4.18.2.28.4. Top Serviços,
4.18.2.28.5. Top origens e os seus principais eventos,
4.18.2.28.6. Top destinos e seus principais eventos;
4.18.2.29. 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;
4.18.2.30. 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.

4.19. ITEM 19 - SOLUÇÃO DE PROTEÇÃO PARA DISPOSITIVOS MÓVEIS ANDROID E IOS

4.19.1. CARACTERÍSTICAS GERAIS
4.19.1.1. A solução deve ser capaz de proteger ameaças de diferentes vetores de ataque, como pelo menos:
4.19.1.1.1. Infecção de Malware;
4.19.1.1.2. Ataques de Phishing;
4.19.1.1.3. Documentos maliciosos;
4.19.1.1.4. Ameaças de rede;
4.19.1.1.5. Alterações ao sistema operacional sem o aviso prévio ao usuário;
4.19.1.2. A solução deve detectar ameaças conhecidas e desconhecidas, incluindo aplicações consideradas de alto risco;
4.19.1.3. A solução deve prevenir o acesso a links maliciosos;

4.19.1.4. A solução de prevenir ataques do tipo phishing e zero-phising (phishing zero-day);
4.19.1.5. A solução deve alertar e bloquear características de side-loading (carregamento em paralelo de aplicações);
4.19.1.6. Suporte para dispositivos BYOD e dispositivos gerenciados dentro da organização;
4.19.1.7. A solução deve suportar os sistemas operacionais Android e iOS;
4.19.1.8. O gerenciamento da solução deve disponibilizar recursos de avaliação de risco completa;
4.19.1.9. O gerenciamento da solução deve disponibilizar ao administrador da solução um dashboard que demonstre, pelo menos:
4.19.1.9.1. O status do risco dos dispositivos
4.19.1.9.2. Status da proteção;
4.19.1.9.3. Eventos e alertas recentes;
4.19.1.10. A solução deve prover opções de remediação e mitigação caso uma ameaça seja detectada;

4.19.2. REQUISITOS DE DETECÇÃO
4.19.2.1. Proteger o dispositivo de aplicações maliciosas conhecidas e desconhecidas.
4.19.2.2. Analisar o comportamento real dos aplicativos.
4.19.2.3. Detectar e analisar o aplicativo baseado na reputação do desenvolvedor.
4.19.2.4. Permitir o Whitelist e Blacklist de aplicações.
4.19.2.5. Prover indicadores de severidade para ameaças identificadas.
4.19.2.6. Prover um SLA (tempo necessário para a detecção de um malware) no momento da sua instalação.
4.19.2.7. A solução deve detectar comunicações comprometidas e tráfego de rede anômalo do dispositivo e para o dispositivo. (Ex. Man-in-The-Middle attack - MiTM)
4.19.2.8. Detecção de interceptação SSL (Ex. SSL string & SSL Bump)
4.19.2.9. Deve possuir habilidade para realizar o Whitelist de certificados.
4.19.2.10. Deve possuir habilidade para configurar URL filter e bloquear o acesso ao recurso quando o dispositivo estiver em risco.
4.19.2.11. Deve possuir habilidade para bloquear o acesso para links maliciosos / sites utilizados para Phishing.
4.19.2.12. 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.
4.19.2.13. Detectar dispositivos Android com Root e dispositivos iOS com Jailbroken habilitados.
4.19.2.14. Detectar ferramentas de evasão para Jailbreak/Root.
4.19.2.15. Alertar sobre exploração de vulnerabilidades utilizando Bluetooth.
4.19.2.16. Detectar configurações de sistema operacional que podem causar risco para o dispositivo.
4.19.2.17. Prevenir mensagens de SMS/Texto que contenham links de phishing.
4.19.2.18. Alertar versões de sistema operacional (OS) desatualizados.
4.19.2.19. Recursos de anti-bot com a capacidade de bloquear malware de realizar acessos a sites, IP e Servidores de C&C maliciosos conhecidos.
4.19.2.20. Bloquear a instalação de profiles de configuração para iOS e permitir a configuração de realizar Whitelist de Profiles.
4.19.2.21. Proteção para aplicativos em execução paralela (background):
4.19.2.22. Gerar alerta no iOS para a aprovação de certificado assinado de desenvolvedor.
4.19.2.23. Habilidade de forçar o scan em aplicativos Android e realizar o bloqueio do APK caso seja identificado como malicioso.
4.19.2.24. Bloquear o download de IPA ou APK (baseado em políticas)
4.19.2.25. Disponibilizar pelo menos 3 níveis de classificação de risco para o dispositivo.
4.19.2.26. A solução deve minimizar a identificação de falso positivo (atribuir risco baixo para aplicativos válidos).

4.19.3. REQUISITOS DE MITIGAÇÃO DE AMEAÇAS

4.19.3.1. 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.
4.19.3.2. 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).
4.19.3.3. 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.
4.19.3.4. A solução deve oferecer a proteção contra ameaças de rede e efetuar o bloqueio a site maliciosos.
4.19.3.5. A solução deve bloquear a comunicação com sites de C&C quando identificado o Malware.
4.19.3.6. A solução deve fornecer suporte para filtro de conteúdo, com bloqueio baseado em categorias para impedir o acesso a sites não autorizados.

4.19.4. REQUISITOS DE INSTALAÇÃO
4.19.4.1. Suporte para a última versão disponível de sistema operacional Android e iOS;
4.19.4.2. O aplicativo deve estar disponibilizado nas lojas oficiais App Store e Google Play.
4.19.4.3. Não permitir alterações na configuração do aplicativo realizadas pelo usuário.
4.19.4.4. Dar suporte para ativação e inicialização remota do aplicativo.
4.19.4.5. Suporte para instalação de aplicativos customizados pela corporação, assinados para iOS.

4.19.5. VISIBILIDADE
4.19.5.1. A solução deve prover total visibilidade e controle sobre os eventos de segurança, e alterações no status do dispositivo.
4.19.5.2. Deve possuir Hhbilidade de conduzir investigações para garantir a aplicação de políticas de segurança contendo as seguintes categorias:
4.19.5.2.1. OS/Dispositivo
4.19.5.2.2. Aplicativos
4.19.5.2.3. Rede
4.19.5.3. A solução deve integrar com soluções de SIEM, suportar o export de logs de Segurança através de Syslog / Remote Syslog.

4.19.6. GERENCIAMENTO E ADMINISTRAÇÃO

4.19.6.1. Possuir um console de gerenciamento unificado;
4.19.6.2. Possuir suporte ao acesso ao console de gerenciamento através de interface web, suportando os navegadores comuns do mercado.
4.19.6.3. Deve possuir configuração de perfis de administrador.
4.19.6.4. A solução deve oferecer suporte granular de configurações através de políticas.
4.19.6.5. O licenciamento deve ser feito por dispositivo protegido;
4.19.6.6. A conexão com a console de gerenciamento deve ser feita através de um protocolo seguro. (Ex: SSL).
4.19.6.7. Habilidade de adicionar ou remover dispositivos, e atribuir a diferentes grupos.
4.19.6.8. 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
4.19.6.9. Permitir a customização do e-mail enviado para os usuários para a instalação e configuração da solução.
4.19.6.10. Deve registrar em logs de auditoria todas as operações dos administradores.
4.19.6.11. Suportar configuração de MFA (Multi Factor Authentication) para o login de administradores a console de gerenciamento.
4.19.6.12. A solução deve suportar integração com soluções MDM / EMM / UEM;
4.19.6.13. A lista de dispositivos a serem provisionados pode ser definida no MDM e lida pela solução;

4.19.6.14. A solução deve listar de dispositivos por agrupamento, conforme apresentado no MDM (por exemplo, estrutura organizacional / etiquetas / etc.);
4.19.6.15. Deve ter a capacidade de bloquear informações pessoais de funcionários do MDM visando privacidade;

4.19.7. RELATÓRIOS E ALERTAS

4.19.7.1. Deve exibir informações sobre a última conexão do agente com a console de gerenciamento por dispositivo.
4.19.7.2. Deve exibir informações sobre o status de provisionamento de cada dispositivo.
4.19.7.3. Deve exibir informações sobre versão do software instalado de cada dispositivo.
4.19.7.4. Deve exibir o número total de dispositivos com o agente instalado na organização.
4.19.7.5. Deve exibir informação sobre os riscos atuais encontrados no dispositivo.
4.19.7.6. Deve exibir informações sobre os tipos de riscos e suas categorias.
4.19.7.7. Deve possuir opção de drill down para a investigação de um alerta específico;
4.19.7.8. Deve possuir alertas de eventos de segurança classificados pelo tipo.
4.19.7.9. Deve possuir alertas de eventos de segurança em filtros diferentes (hora/dia/etc.)
4.19.7.10. Deve possuir habilidade para enviar SMS e e-mail para o administrador referente aos eventos de segurança.
4.19.7.11. Deve permitir a configuração de relatórios agendados de forma diária, semanal ou mensal.

4.19.8. PRIVACIDADE E DESEMPENHO
4.19.8.1. 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.
4.19.8.1.1. Essas informações incluem, mas não se limitam a: mensagens de texto, arquivos de foto / voz / vídeo do dispositivo, outros documentos, e-mails, contatos, eventos da agenda e localização;
4.19.8.2. A solução não deve enviar e armazenar informações de identificação pessoal (PII) para servidores de análise em texto não criptografado;
4.19.8.3. A solução deve ter a capacidade de ocultar a lista de aplicativos por dispositivo por usuário;
4.19.8.4. A solução poderá desativar o rastreamento de localização do dispositivo em ataques à rede por política do cliente;
4.19.8.5. A solução deve ter a capacidade de desativar a leitura de SMS durante ataques de smishing de acordo com a política do cliente;
4.19.8.6. A solução deve permitir gerenciar políticas de segurança por modelo e permitir políticas diferentes para diferentes grupos de dispositivos;
4.19.8.7. 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)
4.19.8.8. A solução deve minimizar o upload de aplicativos para o servidor de análise se o dispositivo estiver usando a rede móvel;

4.19.9. REQUISITOS DE SEGURANÇA

4.19.9.1. A arquitetura da solução deve garantir que nenhuma informação privada de dispositivos e usuários (usuário, nome, e-mail e números de telefone) seja exposta;
4.19.9.2. Todos os protocolos de comunicação entre servidor e cliente devem ser criptografados;
4.19.9.3. Nomes de usuário e senhas armazenados devem ser criptografados;
4.19.9.4. Deve possuiar a capacidade de integração com o Active Directory da organização e permitir acesso SSO (logon único) para os administradores;

4.20. ITEM 20 - SOLUÇÃO DE ACESSO REMOTO SEGURO (SASE)
4.20.1. É permitida a composição da solução ofertada entre diversos fabricantes, desde que não contemple solução de software livre;

4.20.2. Deve ser licenciada pelo número de usuários que utilizarão a plataforma de acesso remoto seguro de borda;
4.20.3. Deve prover acesso a recursos internos (on-premise) ou em múltiplas nuvens sem necessidade do uso de VPN;
4.20.4. Deve permitir acesso com permissões granulares para cada recurso corporativo baseado em permissões dinâmicas e contextuais;
4.20.5. Deve permitir a criação de ilimitadas aplicações;
4.20.6. Deve suportar, no mínimo, os seguintes tipos de aplicações:
4.20.6.1. Web;
4.20.6.2. SSH;
4.20.6.3. RDP;
4.20.6.4. Banco de Dados;
4.20.6.4.1. PostgreSQL;
4.20.6.4.2. MySQL;
4.20.6.4.3. Oracle;
4.20.6.4.4. ElasticSearch;
4.20.6.4.5. MS SQL;
4.20.7. Cada usuário poderá ver, em seu portal, somente as aplicações para as quais possui acesso;
4.20.8. Caso o usuário possua endereço de acesso para uma aplicação para o qual não tem permissão, o acesso deve ser bloqueado pela solução;
4.20.9. A solução não deve depender de cliente instalado na máquina do usuário;
4.20.10. A solução deve permitir a criação de usuários em base de usuários interna;
4.20.11. A gestão interna de usuários deve permitir a criação de usuários e grupos e a configuração de políticas.
4.20.11.1. A autenticação do usuário da base interna de usuários deve ser feita, no mínimo, por usuário e senha;
4.20.12. A solução deve se integrar com bases de identificação externas;
4.20.13. A solução deve ser compatível com, no mínimo, os seguintes provedores de identidade:
4.20.13.1. Okta;
4.20.13.2. AzureAD;
4.20.13.3. ADFS;
4.20.14. Deve ser possível categorizar aplicações através do uso de tags ou pastas;
4.20.15. A categorização deve ser feita, pelo menos, por:
4.20.15.1. Dono;
4.20.15.2. Ambiente;
4.20.16. Deve ser possível personalizar a aplicação web adicionada permitindo o envio de logo da mesma;
4.20.17. A solução deve bloquear todos os links internos da aplicação web de acordo com as melhores práticas da arquitetura Zero-Trust;
4.20.18. Deve permitir acesso completo à aplicação web através de mapeamento dos links de, pelo menos, duas formas:
4.20.18.1. Mapeamento automático: permitir usuários com acesso à aplicação web para utilizar qualquer link dentro da aplicação;
4.20.18.2. Mapeamento manual: adicionar manualmente links permitidos na aplicação web;
4.20.19. Ao adicionar uma aplicação SSH, deve ser possível escolher entre, pelo menos, os seguintes métodos de autenticação:
4.20.19.1. One-time pass: onde os usuários serão fornecidos com uma senha temporária de uso único;
4.20.19.2. Chave privada: o usuário deverá baixar a chave para ter acesso ao recurso SSH;
4.20.20. Deve ser possível configurar a forma como a solução se conectará ao servidor SSH, de, pelo menos, as seguintes formas:
4.20.20.1. Direta: permitir que usuários conectem ao servidor diretamente através da seleção de sua conta e senha;

4.20.20.2. Conta específica: adicionar o servidor com uma conta específica em que todos os usuários serão logados automaticamente;
4.20.21. A solução deve manter logs de atividade de uso das aplicações, servidores e bancos de dados;
4.20.22. Os dados de logs devem ser armazenados em ambiente criptografado e sem exposição para a internet;
4.20.23. Os logs de atividade devem cobrir, pelo menos, as seguintes atividades:
4.20.23.1. Logins efetuados com sucesso;
4.20.23.2. Falha ao efetuar login;
4.20.23.3. Conexão com sucesso às aplicações;
4.20.23.4. Falha em conexão às aplicações;
4.20.23.5. Auditoria de sessões SSH;
4.20.23.6. Mudanças de permissões de usuários;
4.20.23.7. Padrões de acesso;
4.20.23.8. Comportamentos atípicos;
4.20.24. Os logs devem gravar data e hora de cada ocorrência;
4.20.25. Toda a comunicação entre o usuário e a plataforma deve ser realizada através de conexões TLS;

4.21. ITEM 21 – INSTALAÇÃO DE FIREWALL UNIDADE ATÉ 100KM
4.21.1. Instalação e Configuração de Firewall dos itens 1 a 4 em localidade até 100km distante de Fortaleza
4.21.2. A instalação deve ser feita conforme item 2 deste TR.

4.22. ITEM 22 – INSTALAÇÃO DE FIREWALL UNIDADE ATÉ 400KM
4.22.1. Instalação e Configuração de Firewall dos itens 1 a 4 em localidade de 100 km até 400 km distante de Fortaleza
4.22.2. A instalação deve ser feita conforme item 2 deste TR.

4.23. ITEM 23 – INSTALAÇÃO DE FIREWALL UNIDADE ACIMA DE 400KM
4.23.1. Instalação e Configuração de Firewall dos itens 1 a 4 em localidade mais de 400 km distante de Fortaleza
4.23.2. A instalação deve ser feita conforme item 2 deste TR.

4.24. ITEM 24 – INSTALAÇÃO FIREWALL SEDE
4.24.1. Instalação e Configuração de Firewall dos itens 5 a 7;
4.24.2. A instalação deve ser feita conforme item 2 deste TR.

4.25. ITEM 25 – INSTALAÇÃO FIREWALL DATA CENTER
4.25.1. Instalação e Configuração de Firewall dos itens 8 a 10;
4.25.2. A instalação deve ser feita conforme item 2 deste TR.

4.26. ITEM 26 – SERVIÇO DE MONITORAMENTO E SUPORTE TÉCNICO 24X7 DE FIREWALL UNIDADE TIPO 1 E 2 – 36 MESES
4.26.1. Monitoramento e Suporte Técnico 24X7 de Firewall dos itens 1 e 2
4.26.2. O serviço deve ser prestado conforme item 3 deste TR.

4.27. ITEM 27 – SERVIÇO DE MONITORAMENTO E SUPORTE TÉCNICO 24X7 DE FIREWALL UNIDADE TIPO 3 E 4 – 36 MESES
4.27.1. Monitoramento e Suporte Técnico 24X7 de Firewall dos itens 3 e 4
4.27.2. O serviço deve ser prestado conforme item 3 deste TR.

4.28. ITEM 28 – SERVIÇO DE MONITORAMENTO E SUPORTE TÉCNICO 24X7 DE FIREWALL SEDE – 36 MESES

4.28.1. Instalação e Configuração de Firewall dos itens 5 a 7;

4.28.2. O serviço deve ser prestado conforme item 3 deste TR.

4.29. ITEM 29 – SERVIÇO DE MONITORAMENTO E SUPORTE TÉCNICO 24X7 DE FIREWALL DATA CENTER – 36 MESES

4.29.1. Instalação e Configuração de Firewall dos itens 8 a 10;

4.29.2. O serviço deve ser prestado conforme item 3 deste TR.

4.30. ITEM 30 – SERVIÇO DE SOC – SECURITY OPERATIONS CENTER – 24X7 COM SIEM – PACOTES DE 200 EPS – 36 MESES

4.30.1. SERVIÇO DE MONITORAÇÃO E NOTIFICAÇÃO DE INCIDENTES DE SEGURANÇA

4.30.1.1. 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.

4.30.1.2. 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);

4.30.1.3. 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:

4.30.1.3.1. Solução de proteção de endpoints;

4.30.1.3.2. Controle de acesso físico ao SOC, com a utilização de pelo menos 02 (dois) mecanismos de autenticação, sendo, no mínimo, um deles por biometria;

4.30.1.3.3. Monitoramento por sistema interno de TV (CFTV), armazenando as imagens dos últimos 30 (trinta) dias;

4.30.1.3.4. Todos os funcionários da CONTRATADA envolvidos na operação ou que possuam acesso às informações do CONTRATANTE devem assinar termo de responsabilidade e sigilo;

4.30.1.4. 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);

4.30.1.5. 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;

4.30.1.6. A CONTRATADA é responsável pelas atividades de camada 1 do SOC, que para o modelo definido corresponde minimamente às atividades relacionadas abaixo:

4.30.1.6.1. 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

4.30.1.6.2. 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 desenvolvida, podendo passar a utilizar múltiplos eventos e diferentes fontes de dados. Os alertas devem indicar minimamente:

4.30.1.6.2.1. Ataques de força bruta com e sem sucesso;

4.30.1.6.2.2. Falhas de autenticação que indiquem suspeita de roubo de identidade;

4.30.1.6.2.3. Infecção de equipamentos por vírus;

4.30.1.6.2.4. Comprometimento de ativos da rede;
4.30.1.6.2.5. Realização de ações suspeitas por parte de usuários privilegiados;
4.30.1.6.2.6. Alertas de operação de serviços, como interrupções e falhas;
4.30.1.6.2.7. Ataques de negação de serviço;
4.30.1.6.2.8. Ataques comuns em aplicações WEB, como XSS e SQL injection;
4.30.1.6.2.9. Atividades de botnets;
4.30.1.6.2.10. Exploração de vulnerabilidades;
4.30.1.6.3. 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.
4.30.1.6.4. 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 seguintes categorias:
4.30.1.6.4.1. Evento confirmado: os sensores detectaram corretamente uma ameaça válida. Os incidentes confirmados devem ser escalados para a etapa de mitigação da gestão de incidentes;
4.30.1.6.4.2. 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;
4.30.1.6.4.3. Eventos autorizados: são ameaças detectadas corretamente, mas que são aprovadas pela política de segurança, como por exemplo, a análise de vulnerabilidades;
4.30.1.6.4.4. Indeterminado: quando não existe evidência suficiente para confirmar o evento de segurança;
4.30.1.6.5. 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:
4.30.1.6.5.1. Identificador do ticket;
4.30.1.6.5.2. Sensor que detectou o evento;
4.30.1.6.5.3. Identificador do evento gerado no sensor;
4.30.1.6.5.4. Limiar de detecção utilizado para enviar o evento para análise;
4.30.1.6.5.5. Log do evento detectado;
4.30.1.6.5.6. Origem e categoria do ataque;
4.30.1.6.5.7. Data e hora;

4.30.1.6.6. 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;
4.30.1.6.7. Elaboração de relatórios. A CONTRATADA deverá disponibilizar relatórios em formato pdf, referentes aos indicadores monitorados com periodicidade mínima mensal, ou sob demanda, podendo incluir:
4.30.1.6.7.1. Classificação dos eventos de segurança;
4.30.1.6.7.2. Total de eventos avaliados;
4.30.1.6.7.3. Total de eventos escalados;
4.30.1.6.7.4. TOP aplicações mais impactadas, TOP origens dos eventos de segurança;
4.30.1.6.7.5. TOP endereços de destino das ameaças;
4.30.1.6.7.6. TOP URLs e suas categorias;
4.30.1.6.7.7. TOP atacantes, vulnerabilidades, ameaças, alarmes, violações de auditoria;
4.30.1.6.7.8. Principais tipos de ataques;
4.30.1.6.7.9. Descrição dos casos de uso utilizados para avaliar os alertas de segurança;
4.30.1.6.7.10. Novas informações de inteligência configuradas na ferramenta: como as novas regras de monitoramento, dashboards, assinaturas instaladas, etc;

4.30.1.6.8. 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;
4.30.1.6.9. 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;
4.30.1.6.10. Os analistas do CONTRATANTE responsáveis pelos tíquetes escalados devem possuir acesso total as informações do incidente relacionado;
4.30.1.6.11. 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;
4.30.1.6.12. 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;
4.30.1.6.13. 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;
4.30.1.6.14. 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 segurança. 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;
4.30.1.6.15. 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;

4.30.2. CARACTERÍSTICAS E REQUISITOS INDISPENSÁVEIS PARA OS SERVIÇOS E RECURSOS FORNECIDOS PELO SECURITY OPERATIONS CENTER (SOC):

4.30.2.1. CORRELACIONAMENTO DE EVENTOS DE SEGURANÇA DA INFORMAÇÃO
4.30.2.1.1. 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;
4.30.2.1.2. A solução deverá ser fornecida para instalação e uso no idioma Português Brasil e Inglês;
4.30.2.1.3. A solução deverá ter o pleno funcionamento independentemente de conexão (física ou lógica) com o fabricante;
4.30.2.1.4. A solução deve sincronizar o horário de seus componentes utilizando o serviço NTP;
4.30.2.1.5. A solução deve ser gerenciada centralmente (configurações, controle e atualizações), através de interface web única, sem necessidades de intervenção nos equipamentos onde está instalado;

4.30.2.1.6. 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;
4.30.2.1.7. A solução deve permitir a recepção de eventos que excedam temporariamente os limites contratados, 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;
4.30.2.1.8. A comunicação entre os componentes da solução deverá ser feita de forma criptografada, garantindo a autenticidade, confidencialidade e integridade dos dados;
4.30.2.1.9. 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;
4.30.2.1.10. Ter suporte a monitoração por SNMPv2c e SNMPv3;
4.30.2.1.11. A administração da solução deve usar uma única conta para cada usuário administrador (mesma conta, mesma senha), independente da funcionalidade gerenciada;
4.30.2.1.12. A coleta, normalização e o correlacionamento dos eventos provenientes dos dispositivos monitorados devem ser realizadas próximos ao tempo real;
4.30.2.1.13. Os eventos devem ser normalizados e categorizados em um padrão único que será usado pela solução;
4.30.2.1.14. 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;
4.30.2.1.15. Propriedades customizadas devem poder ser usadas em regras de correlação online e em regras de correlação histórica;
4.30.2.1.16. Permitir a agregação de eventos semelhantes;
4.30.2.1.17. Deve atribuir métrica de prioridade para os eventos e para os alertas/incidentes;
4.30.2.1.18. Gerar alertas/incidentes com base nas regras definidas previamente;
4.30.2.1.19. Verificar conformidade com as políticas, controles e normas internas (customizadas) e regulamentações externas (ex. ISO 27001);
4.30.2.1.20. Deve permitir armazenar os eventos, inclusive os normalizados, de forma compactada;
4.30.2.1.21. Apresentar painéis gráficos (dashboards) com indicativos de situações relacionados à segurança, compliance, aplicações e monitoração do próprio sistema;
4.30.2.1.22. Os painéis gráficos (dashboards) devem ser customizáveis, por usuário;
4.30.2.1.23. Permitir a análise de eventos baseados em contexto, tais como, usuários, localização geográfica, bem como qualquer outro metadado contido no evento;
4.30.2.1.24. Enviar notificações relacionadas a um incidente/alerta por e-mail, trap snmp e syslog;
4.30.2.1.25. 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 Protocol;
4.30.2.1.26. Deve permitir a configuração de ofuscação de qualquer parte dos dados recebidos, assim que normalizados;
4.30.2.1.27. A ofuscação de dados deve ser configurada com chaves de criptografia;
4.30.2.1.28. Possuir a capacidade de automatizar a resposta a incidentes, através da execução de scripts, como ação customizada dentro das regras de correlação;
4.30.2.1.29. Tratar eventos em formato “comprimido” (zip, gz, tar.gz), sem a necessidade da descompressão manual;
4.30.2.1.30. 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;
4.30.2.1.31. Deve manter o evento bruto (“raw”) e seus metadados para o armazenamento e consulta futura;

4.30.2.1.32. Deve ser capaz de agregar informações sobre localização geográfica dos endereços IP envolvidos no evento, para que a mesma seja usada no correlacionamento;
4.30.2.1.33. 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);
4.30.2.1.34. 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;
4.30.2.1.35. Deve exibir perfil visual do tráfego em tempo real, e normalizada de forma agregada. Deve incluir informações de bytes, pacotes e protocolos;
4.30.2.1.36. 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;
4.30.2.1.37. Deve possuir mecanismo para não sofrer as consequências da monitoração de flows de rede em uma situação de DDoS;
4.30.2.1.38. 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;
4.30.2.1.39. 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;
4.30.2.1.40. Deve ser capaz de apresentar informações de fluxo de rede por período de tempo pré-definido;
4.30.2.1.41. Deve ser capaz de montar visualizações de fluxo de rede baseados em comunicações provenientes ou destinadas à internet agrupado por regiões geográficas;
4.30.2.1.42. Deve correlacionar logs e flows em conjunto, gerando incidentes de segurança;
4.30.2.1.43. Deve possuir regras de correlação específicas para regulações/conformidades, com suporte no mínimo a: ISO 27001 e GDPR/LGPD;
4.30.2.1.44. 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;
4.30.2.1.45. 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);
4.30.2.1.46. 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;
4.30.2.1.47. Possuir pelo menos os seguintes tipos de correlação:
4.30.2.1.47.1. Correlação por regras;
4.30.2.1.47.2. Extrapolação de um limite (threashold);
4.30.2.1.47.3. Correlação por anomalia e padrão de comportamento;
4.30.2.1.48. 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 listas (watch list);
4.30.2.1.49. 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;
4.30.2.1.50. Qualquer metadado dos eventos pode ser usado em uma regra de correlação;
4.30.2.1.51. 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;
4.30.2.1.52. 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;
4.30.2.1.53. Identificação de ações que comprometam dados cobertos pelas regulações LGPD (Lei Geral de Proteção a Dados) ou GDPR (General Data Protection Regulation);
4.30.2.1.54. Comunicação dos equipamentos internos com sites conhecidos por serem controladores de botnet;

4.30.2.1.55. Deve permitir o uso de algoritmo para garantia de integridade dos eventos armazenados, utilizando no mínimo os algoritmos: MD2, MD5, SHA-256, SHA-384 e SHA-512;
4.30.2.1.56. Deve permitir o uso dos algoritmos para garantia de integridade, do item anterior, com código de autenticação da mensagem (HMAC);
4.30.2.1.57. 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;
4.30.2.1.58. 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;
4.30.2.1.59. Possuir capacidade de integração com bases Microsoft Active Directory, LDAP, TACACS e RADIUS para autenticação de usuários;
4.30.2.1.60. Deve permitir a integração com Single Sign-On que suporte o protocolo SAML 2.0;
4.30.2.1.61. 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;
4.30.2.1.62. Capacidade de criação de novos painéis gráficos (dashboards) e alteração dos existentes;
4.30.2.1.63. 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;
4.30.2.1.64. Permitir agendar a geração de relatórios de forma periódica e notificar/enviar automaticamente os relatórios gerados para os destinatários dos mesmos;
4.30.2.1.65. Deve possuir templates de relatórios para as principais normas de conformidade. Sendo exigido, no mínimo, o atendimento a ISO/27001;
4.30.2.1.66. 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;
4.30.2.1.67. Deve permitir a geração de relatórios, contendo múltiplas informações num mesmo relatório, como dados de segurança e rede;
4.30.2.1.68. Deve permitir a criação de relatórios relacionados a: incidentes, logs, flows de rede, vulnerabilidades;
4.30.2.1.69. 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;
4.30.2.1.70. Deve possuir módulo capaz de extrair os dados de usuário e ações executadas dos eventos coletados para geração de score de risco;
4.30.2.1.71. 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;

4.31. DAS CONDIÇÕES DE INSTALAÇÃO

4.31.1. É/será de inteira responsabilidade da CONTRATADA a correta instalação, configuração e funcionamento dos equipamentos e componentes da solução ofertada, caso um dos serviços de instalação (itens 20 a 24) 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.
4.31.2. A instalação e configuração dos equipamentos será de responsabilidade da CONTRATANTE caso nenhum dos itens 21 a 25 seja contratado.
4.31.3. Em processos de implantação de Firewall CENTRAL (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:
4.31.3.1. 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;

4.31.3.2. 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.;
4.31.3.3. 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;
4.31.3.4. 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;
4.31.3.5. Ao término dos serviços deve ser criado um relatório detalhado contendo todos os itens configurados 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;
4.31.3.6. 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;
4.31.4. Em processos de implantação de até 10 unidades de Firewall UNIDADE REMOTA (itens 1 a 4) os processos detalhados em 2.3 podem ser executados de maneira simplificada sendo, no entanto, obrigatório:
4.31.4.1. 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;
4.31.4.2. Relatório as-built simplificado;
4.31.4.3. Documentação completa da solução, incluindo especificação do equipamento, características e funcionalidades implementadas, comentários e configurações executadas.

4.32. DAS CONDIÇÕES DE SUPORTE E ASSISTÊNCIA TÉCNICA 24X7

4.32.1. A Licitante Vencedora deverá apresentar juntamente a sua Proposta uma Carta de cada Fabricante do item proposto declarando que seja Revenda Autorizada/Parceiro e empresa capacitada como Prestadora de Serviços do Fabricante.
4.32.2. A CONTRATADA dará suporte e assistência técnica 24X7 conforme descrito abaixo caso um dos itens 26 a 29 seja contratado, pelo período de 36 (trinta e seis) meses.
4.32.3. O suporte e assistência técnica se dará conforme as condições especificadas no item 4 deste TR caso nenhum dos itens 26 a 29 seja contratado.
4.32.4. A CONTRATADA deverá possuir uma solução de monitoramento conforme Anexo B.
4.32.5. 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.
4.32.6. 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 comtemplado nesse Edital. As tarefas atinentes ao transporte, deslocamento e remessa necessários, seja na implementação, substituição e/ ou remoção de equipamentos defeituosos será de responsabilidade da CONTRATADA.

4.32.7. 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 B. Essas características deverão constar na comprovação ponto-a-ponto que será entregue.
4.32.8. A ferramenta deve ser acompanhada de todos os itens necessários para operacionalização, tais como: softwares de apoio (sistema operacional, etc) e licenças de softwares;
4.32.9. 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.
4.32.10. Os serviços prestados pelo NOC compreendem, entre outros, os seguintes procedimentos:
4.32.11. Monitoramento pró-ativo do ambiente de rede WAN do CONTRATANTE;
4.32.12. Suporte técnico para identificação e resolução de problemas em software e hardware;
4.32.13. Resolução de problemas quanto acesso à internet, sites remotos, serviços de rede oferecidos aos funcionários do CONTRATANTE;
4.32.14. Resolução de problemas referente aos meios de Acesso WAN, tais como: MPLS e Ethernet;
4.32.15. Suporte em criação de políticas, configurações, parametrizações de quaisquer ordens relativos aos equipamentos ofertados;
4.32.16. Resolução de problemas referente a políticas, configurações, parametrizações de quaisquer ordens relativos aos equipamentos ofertados;
4.32.17. Suporte à criação, geração e parametrização de relatórios e eventos de segurança de quaisquer naturezas detectados e prevenidos pelos equipamentos ofertados;
4.32.18. Encaminhar incidentes ao fabricante da solução;
4.32.19. Suporte em demais configurações de segurança, redundância e gerência;
4.32.20. Suporte, administração e monitoramento das políticas e tarefas de backup das configurações;
4.32.21. Apoio técnico para tarefas de auditoria e análise de logs.
4.32.22. 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.
4.32.23. O atendimento e suporte técnico especializado de 1º (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.
4.32.24. O atendimento e suporte técnico especializado de 2º (segundo nível) poderá ser presencial 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.
4.32.25. 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.
4.32.26. 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.

4.32.27. 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:
4.32.28. 02 (dois) profissionais com nível professional na solução ofertada
4.32.29. 02 (dois) profissionais com nível expert na solução ofertada;
4.32.30. 02 (dois) profissionais com certificação ITIL Foundation;
4.32.31. 01 (um) profissional com certificação PMP;
4.32.32. 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.
4.32.33. 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 operação do serviço).
4.32.34. 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 equipamentos ou componentes substituídos, especificando marca, modelo, fabricante e número de série).
4.32.35. 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.
4.32.36. 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.
4.32.37. 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.
4.32.38. 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:
4.32.39. Operação parada (incidente que gere parada total de algum serviço contemplado nesse contrato) o tempo de atendimento será de até 2 (duas) horas.
4.32.40. Operação impactada (incidente que gere parada parcial de algum serviço contemplado nesse contrato) o tempo de atendimento será de até 4 (quatro) horas.
4.32.41. Requisição de serviço (solicitações de mudanças nos equipamentos ou serviços do contrato) o tempo de atendimento será de até 8 (oito) horas.
4.32.42. 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.

4.33. DAS CONDIÇÕES DE GARANTIA, SUPORTE E ASSISTÊNCIA TÉCNICA

4.33.1. Os itens 1 a 20, deste TR devem oferecer as condições de garantia conforme descrito abaixo.
4.33.2. 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.

4.33.3. 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;

4.33.4. 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.

5. DOS RECURSOS ORÇAMENTÁRIOS

5.1. As despesas decorrentes da Ata de Registro de Preços, correrão pela fonte de recursos da ETICE e do(s) órgão(s)/entidade(s) participante(s) do SRP (Sistema de Registro de Preços), a ser informada quando da lavratura do contrato.

6. DA ENTREGA E DO RECEBIMENTO

6.1. Quanto à entrega:

6.1.1. Os itens 1 a 20 deverão ser entregues em conformidade com as especificações estabelecidas neste instrumento, em um prazo máximo de 90 (noventa) dias úteis contados a partir do recebimento da ordem de serviço ou instrumento hábil.

6.1.2. O objeto contratual deverá ser entregue em conformidade com as especificações estabelecidas neste instrumento. O Local de entrega e os endereços específicos de cada localidade beneficiada serão repassados pela CONTRATANTE a CONTRATADA, de acordo com o estabelecido na Ordem de Serviço.

6.1.3. Os atrasos ocasionados por motivo de força maior ou caso fortuito, desde que justificados até 2 (dois) dias úteis antes do término do prazo de execução, e aceitos pela CONTRATANTE, não serão considerados como inadimplemento contratual.

6.2. Quanto ao recebimento:

6.2.1. PROVISORIAMENTE, mediante recibo, para efeito de posterior verificação da conformidade do objeto com as especificações, devendo ser feito por pessoa credenciada pela CONTRATANTE.

6.2.2. DEFINITIVAMENTE, sendo expedido termo de recebimento definitivo, após a verificação da qualidade e quantidade do objeto, certificando-se de que todas as condições estabelecidas foram atendidas e consequente aceitação das notas fiscais pelo gestor da contratação, devendo haver rejeição no caso de desconformidade.

7. DO PAGAMENTO

7.1. O pagamento advindo do objeto da Ata de Registro de Preços será proveniente dos recursos do (s) próprios órgão (s)/entidades participante (s) e será efetuado mensalmente até 30 (trinta) dias a contar da data da apresentação da Nota Fiscal/Fatura devidamente atestada pelo gestor da contratação, mediante crédito em conta corrente em nome da contratada, exclusivamente no Banco Bradesco S/A, conforme Lei nº 15.241, de 06 de dezembro de 2012, salvo as economias mistas e suas subsidiárias com exceção da Companhia de Água e Esgoto – CAGECE.

7.2. A nota fiscal/fatura que apresente incorreções será devolvida à contratada para as devidas correções. Nesse caso, o prazo de que trata o subitem anterior começará a fluir a partir da data de apresentação da nota fiscal/fatura corrigida.

7.3. No caso dos itens 26 a 29 o pagamento será realizado mensalmente referente a quantidade de itens que estão sendo monitorados e/ou mantidos.

7.4. Não será efetuado qualquer pagamento à CONTRATADA, antes da execução do objeto, se o objeto não estiver de acordo com as especificações deste instrumento e em caso de descumprimento das condições de habilitação exigidas na licitação.

7.5. No caso de atraso de pagamento, desde que a contratada não tenha concorrido de alguma forma para tanto, serão devidos pela contratante encargos moratórios à taxa nominal de 6% a.a. (seis por cento ao ano), capitalizados diariamente em regime de juros simples.
7.6. O valor dos encargos será calculado pela fórmula: EM = I x N x VP, onde: EM = Encargos moratórios devidos, N = Números de dias entre a data prevista para o pagamento e a do efetivo pagamento, I = Índice de compensação financeira = 0,00016438 e VP = Valor da prestação em atraso.
7.7. Os pagamentos encontram-se ainda condicionados à apresentação dos seguintes comprovantes:
7.8. Certidão Conjunta Negativa de Débitos relativos aos Tributos Federais e à Dívida Ativa da União, Certidão Negativa de Débitos Estaduais, Certidão Negativa de Débitos Municipais, Certificado de Regularidade do FGTS - CRF, Certidão Negativa de Débitos Trabalhistas - CNDT.
7.9. Toda a documentação exigida deverá ser apresentada em original ou por qualquer processo de reprografia, autenticada por cartório competente ou por servidor da Administração, ou publicação em órgão da imprensa oficial. Caso a documentação tenha sido emitida pela internet, só será aceita após a confirmação de sua autenticidade.

8. DAS SANÇÕES ADMINISTRATIVAS

8.1. Das estatais:

Pela inexecução total ou parcial do contrato, a ETICE poderá, garantida a prévia defesa, aplicar a contratada, nos termos do art. 83 da Lei nº 13.303/2016 e dos arts. 166 a 169 do seu Regulamento de Licitações e Contratos, as seguintes penalidades:
8.1.1.Advertência

8.1.1.2. Multas, estipuladas na forma a seguir:

a) Multa de 0,07% (sete centésimos por cento) do valor do contrato, por dia de atraso, até o máximo de 2% (dois por cento) pela inobservância do prazo fixado para apresentação da garantia.
b) Multa diária de 0,3% (três décimos por cento), no caso de atraso na execução do objeto contratual até o 30º (trigésimo) dia sobre o valor da nota de empenho ou instrumento equivalente.
c) Multa diária de 0,5% (cinco décimos por cento), no caso de atraso na execução do objeto contratual superior a 30 (trinta) dias, sobre o valor da nota de empenho ou instrumento equivalente até o limite do percentual fixado na alínea “e”, hipótese que pode resultar na rescisão da avença. A aplicação da presente multa exclui a aplicação da multa prevista na alínea anterior.
d) Multa diária de 0,1% (um décimo por cento) sobre o valor da nota de empenho ou instrumento equivalente em caso de descumprimento das demais cláusulas contratuais, elevada para 0,3% (três décimos por cento) em caso de reincidência.
e) Multa de 20% (vinte por cento) sobre o valor do contrato, no caso de desistência da execução do objeto ou rescisão contratual não motivada pela contratante, inclusive o cancelamento do registro de preço.

8.1.1.3. Suspensão temporária de participação em licitação e impedimento de contratar com a entidade sancionadora, por prazo não superior a 2 (dois) anos.
8.1.2. Se não for possível o pagamento da multa por meio de descontos dos créditos existentes, a contratada recolherá a multa por meio de depósito bancário em nome da contratante, se não o fizer, será cobrada em processo de execução.

8.2. Dos demais órgãos da administração pública

8.2.1. No caso de inadimplemento de suas obrigações, a contratada estará sujeita, sem prejuízo das sanções legais nas esferas civil e criminal, às seguintes penalidades:

8.2.1.1. Multas, estipuladas na forma a seguir:

a) Multa de 0,07% (sete centésimos por cento) do valor do contrato, por dia de atraso, até o máximo de 2% (dois por cento) pela inobservância do prazo fixado para apresentação da garantia.

b) Multa diária de 0,3% (três décimos por cento), no caso de atraso na execução do objeto contratual até o 30º (trigésimo) dia, sobre o valor da nota de empenho ou instrumento equivalente.

c) Multa diária de 0,5% (cinco décimos por cento), no caso de atraso na execução do objeto contratual superior a 30 (trinta) dias, sobre o valor da nota de empenho ou instrumento equivalente, até o limite do percentual fixado na alínea “e”, hipótese que pode resultar na rescisão da avença. A aplicação da presente multa exclui a aplicação da multa prevista na alínea anterior.

d) Multa diária de 0,1% (um décimo por cento) sobre o valor da nota de empenho ou instrumento equivalente, em caso de descumprimento das demais cláusulas contratuais, elevada para 0,3% (três décimos por cento) em caso de reincidência.

e) Multa de 20% (vinte por cento) sobre o valor do contrato, no caso de desistência da execução do objeto ou rescisão contratual não motivada pela contratante, inclusive o cancelamento do registro de preço.

8.2.1.2.Impedimento de licitar e contratar com a Administração, sendo então, descredenciada no cadastro de fornecedores da Secretaria do Planejamento e Gestão (SEPLAG), do Estado do Ceará, pelo prazo de até 5 (cinco) anos, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, sem prejuízo das multas previstas neste instrumento e das demais cominações legais.

8.3. A multa a que porventura a contratada der causa será descontada da garantia contratual ou, na sua ausência, insuficiência ou de comum acordo, nos documentos de cobrança e pagamento pela execução do contrato, reservando-se a contratante o direito de utilizar, se necessário, outro meio adequado à liquidação do débito.

8.3.1 Se não for possível o pagamento da multa por meio de descontos dos créditos existentes, a CONTRATADA 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.

8.4. A multa poderá ser aplicada com outras sanções segundo a natureza e a gravidade da falta cometida, desde que observado o princípio da proporcionalidade.

8.5. Nenhuma sanção será aplicada sem garantia da ampla defesa e contraditório, na forma da lei.

9. DAS OBRIGAÇÕES DA CONTRATADA

9.1. Executar o objeto em conformidade com as condições deste instrumento.

9.2. Manter durante toda a execução contratual, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

9.3. Aceitar, nas mesmas condições contratuais, os percentuais de acréscimos ou supressões limitados ao estabelecido no § 1º, do art. 65, da Lei Federal nº 8.666/1993, tomando-se por base o valor contratual.

9.4.Responsabilizar-se pelos danos causados diretamente à contratante ou a terceiros, decorrentes da sua culpa ou dolo, quando da execução do objeto, não podendo ser arguido para efeito de exclusão ou redução de sua responsabilidade o fato de a contratante proceder à fiscalização ou acompanhar a execução contratual.

9.5. Responder por todas as despesas diretas e indiretas que incidam ou venham a incidir sobre a execução contratual, inclusive as obrigações relativas a salários, previdência social, impostos, encargos sociais e outras providências, respondendo obrigatoriamente pelo fiel cumprimento das leis trabalhistas e específicas de acidentes do trabalho e legislação correlata, aplicáveis ao pessoal empregado na execução contratual. A inadimplência da contratada quanto aos encargos trabalhistas, fiscais e comerciais não transfere à CONTRATANTE a responsabilidade por seu pagamento, nem poderá onerar o objeto do contrato.

9.6 Prestar imediatamente as informações e os esclarecimentos que venham a ser solicitados pela contratante, salvo quando implicarem em indagações de caráter técnico, hipótese em que serão respondidas no prazo de 24 (vinte e quatro) horas.

9.7. Refazer, substituir ou reparar o objeto contratual que comprovadamente apresente condições de defeito ou em desconformidade com as especificações deste termo, no prazo fixado pelo (s) órgão (s) /entidade (s) participante (s) do SRP (Sistema de Registro de Preços), contado da sua notificação.

9.8. Cumprir, quando for o caso, as condições de garantia do objeto, responsabilizando-se pelo período oferecido em sua proposta comercial, observando o prazo mínimo exigido pela Administração.

9.9. Providenciar a substituição de qualquer empregado que esteja a serviço da contratante, cuja conduta seja considerada indesejável pela fiscalização da contratante.

9.10. Responsabilizar-se integralmente pela observância do dispositivo no título II, capítulo V, da CLT, e na Portaria nº 3.460/77, do Ministério do Trabalho, relativos a segurança e higiene do trabalho, bem como a Legislação correlata em vigor a ser exigida.

9.11. Respeitar a legislação relativa à disposição final ambientalmente adequada dos resíduos gerados, mitigação dos danos ambientais por meio de medidas condicionantes e de compensação ambiental e outros, conforme previsto em lei.

9.12. Disponibilizar nos termos da Lei nº 15.854, de 24/09/2015, vagas de empregos a presos em regime semiaberto, aberto, em livramento condicional e egressos do sistema prisional e aos jovens do sistema socioeducativo entre 16 e 18 anos, que estejam cumprindo medida de semiliberdade. Caso a execução contratual não necessite, ou necessite de 5 (cinco) ou menos trabalhadores, a reserva de vagas será facultativa.

9.12.1.Encaminhar mensalmente, respectivamente, à CISPE/SEJUS e à SPS, a folha de frequência dos presos e egressos e/ou jovens do sistema socioeducativo, contemplados com a reserva de vagas. Caso a contratação não esteja obrigada a disponibilizar vagas nos termos da Lei nº 15.854, de 24/09/2015 ficará dispensada do envio da folha de frequência.

10. DAS OBRIGAÇÕES DA CONTRATANTE

10.1. Solicitar a execução do objeto à contratada através da emissão de Ordem de Fornecimento/ Serviço.

10.2. Proporcionar à contratada todas as condições necessárias ao pleno cumprimento das obrigações decorrentes do objeto contratual, consoante estabelece a Lei Federal no 13.303/2016, no caso das estatais e a Lei Federal n° 8.666/1993 para os demais órgãos/entidades.

10.3. Fiscalizar a execução do objeto contratual, através de sua unidade competente, podendo, em decorrência, solicitar providências da contratada, que atenderá ou justificará de imediato.

10.4. Notificar a contratada de qualquer irregularidade decorrente da execução do objeto contratual.

10.5. Efetuar os pagamentos devidos à contratada nas condições estabelecidas neste Termo.

10.6. Aplicar as penalidades previstas em lei e neste instrumento.

11. DA FISCALIZAÇÃO

11.1. A execução contratual será acompanhada e fiscalizada, por um representante especialmente designado para este fim pela contratante, de acordo com o estabelecido no art. 67, da Lei Federal nº 8.666/1993, a ser informado quando da lavratura do instrumento contratual, e no caso das estatais, conforme disposto nos seus respectivos Regulamentos Internos de Licitações e Contratos.

12. PRAZO DE VIGÊNCIA DA ATA DE REGISTRO DE PREÇOS

12.1. Ata de Registro de Preços terá validade pelo prazo de 12 (doze) meses, contados a partir da data da sua publicação ou então até o esgotamento do quantitativo nela registrado, se este ocorrer primeiro.

13. DA GERÊNCIA DA ATA DE REGISTRO DE PREÇOS

13.1. Caberá à Empresa de Tecnologia da Informação do Ceará - ETICE o gerenciamento da Ata de Registro de Preços, no seu aspecto operacional e nas questões legais, em conformidade com as normas do Decreto Estadual nº 32.824/2018, publicado no DOE de 11/10/2018.

14. PRAZO DE VIGÊNCIA E DE EXECUÇÃO DO CONTRATO

14.1. Os prazos de vigência e de execução contratual obedecerão ao disposto abaixo:

14.1.1. Em caso de contratação dos itens 1 a 25, os prazos de vigência e de execução contratual serão de 12 (doze) meses, contados a partir do recebimento da ordem de serviço, e para as empresas públicas, economia mistas e suas subsidiárias, a partir da celebração do contrato conforme disposto no art. 71 da Lei nº 13.303/2016.

14.1.2. Em caso de contratação dos itens 26 a 30, os prazos de vigência e de execução contratual serão de 36 (trinta e seis) meses, contados a partir do recebimento da ordem de serviço, e para as empresas

públicas, economia mistas e suas subsidiárias, a partir da celebração do contrato conforme disposto no art. 71 da Lei nº 13.303/2016.

14.2. Os prazos de vigência e de execução contratual poderão ser prorrogados e alterados, respectivamente nos termos do art. 71 e art. 81 da Lei Federal nº 13.303/2016, e do Regulamento Interno de Licitações e Contratações das para as empresas públicas e sociedades de economia mista e nos termos do art. 57, § 1º e art. 65 da Lei Federal n° 8.666/1993, para os demais órgãos/entidades da administração pública.

14.3. A publicação resumida do contrato dar-se-á na forma do § 2º do art. 51 da Lei nº 13.303/2016 para as empresas públicas e sociedades de economia mista e nos termos do parágrafo único, do art. 61, da Lei Federal nº 8.666/1993, para os demais órgãos/entidades da administração pública.

15. DOS ANEXOS DO TERMO DE REFERÊNCIA

ANEXO A - Especificações da Solução de Gerência Centralizada e Relatoria
ANEXO B – PLATAFORMA DE MONITORAMENTO
ANEXO C - ÓRGÃO(S) PARTICIPANTE(S)
ANEXO D – SUMÁRIO DE COMPROVAÇÕES TÉCNICAS

ANEXO A - 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 10 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 configuração da regra selecionada;
16. Deve possibilitar a integração com outras soluções de SIEM de mercado desde que não sejam software livre;
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;
33. 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;
34. 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.;
35. A solução deve prover, no mínimo, as seguintes funcionalidades para análise avançada dos incidentes:
36. Visualizar quantidade de tráfego utilizado de aplicações e navegação;
37. Gráficos com principais eventos de segurança de acordo com a funcionalidade selecionada;
38. A solução de correlação deve possuir mecanismo para detectar login de administradores em horários irregulares;
39. A solução deve ser capaz de detectar ataques de tentativa de login e senha utilizando tipos diferentes de credencias;
40. Deve suportar a geração de relatório gerencial para apresentar aos executivos os eventos de ataque de forma completamente visual, utilizando, para tanto, gráficos, consumo de banda utilizado pelos ataques e quantidade de eventos gerados e protegidos;
41. Deve permitir a integração com servidores de autenticação LDAP Microsoft Active Directory e Radius;
42. Permitir criações de políticas de acesso de usuários autenticada no Active Directory, de forma que reconheça os usuários de forma transparente;
43. Permitir o download de assinaturas, atualizações e firmwares para distribuição centralizada aos dispositivos de segurança integrados a mesma;
44. Permitir a visualização de gráficos e mapa de ameaças;
45. Possuir mecanismo para que logs antigos sejam removidos automaticamente;
46. Deve permitir a criação de dashboards customizados para visibilidades do tráfego de aplicativos, categorias de URL, ameaças, serviços, países, origem e destino;
47. Deve possuir a capacidade de visualizar na interface gráfica da solução, informações do sistema como licenças, memória, disco e uso de CPU;
48. A solução deve ser capaz de correlacionar eventos de todas as fontes de log em tempo real;
49. A solução deve fornecer conteúdo de correlação pré-definido organizado por categoria;
50. A solução deve possuir painéis de eventos em tempo real com possibilidade de configuração das atualizações e frequências;

ANEXO B – 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 Explorer.
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 seguintes 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 inferfaces 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 pré-agendar 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 parada perante os demais objetos monitorados;

ANEXO C – ÓRGÃO PARTICIPANTE

Seq.	Órgãos/Entidades	ENDEREÇO
1	Empresa de Tecnologia da Informação do Ceará - ETICE	Av. Pontes Vieira, 220 - São João do Tauape. CEP: 60.130-240. Fortaleza-CE.

ANEXO D – SUMÁRIO DE COMPROVAÇÕES 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 arrematante, 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). Declarações do fabricante ou do licitante só serão aceitas em casos que seja claro a impossibilidade de usar outro tipo de comprovação. 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 tabela ilustrativa abaixo exemplifica como as Comprovações Técnicas deverão ser apresentadas. O exemplo apresentado para o item 4.1.1 deve ser usado na comprovação do atendimento a todas as especificações técnicas para os equipamentos e soluções constantes no Termo de Referência do Edital (itens 1 ao 20, e item 30) que abrangem a numeração 4.1.1 a 4.30.2.1.71. do Termo de Referência e Anexos A e B do Termo de Referência.

Item	Descrição	Documento	Página
4.1.1.	**ITEM 1 – NEXT GENERATION FIREWALL – UNIDADE TIPO I**	---	----
4.1.2.	**CARACTERÍSTICAS GERAIS**	---	----
4.1.2.1.	É permitida a composição da solução ofertada entre diversos fabricantes, desde que não contemple solução de software livre;	Catálogo X	1 a 5
4.1.2.2.	A solução deverá ser compatível com SNMPv2 e SNMPv3;	Catálogo Y	1 a 2
	…….		

ANEXO II - CARTA PROPOSTA

À
Central de Licitações do Estado do Ceará.
Ref.: Pregão Eletrônico nº 20210007– ETICE.

A proposta encontra-se em conformidade com as informações previstas no edital e seus Anexos.

1. Identificação do licitante:

a) Razão Social:
b) CPF/CNPJ e Inscrição Estadual:
c) Endereço completo:
d) Representante Legal (nome, nacionalidade, estado civil, profissão, RG, CPF, domicílio):
e) 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	UNIDADE	QTDE	VALOR (R$)	
				UNITÁRIO	TOTAL
VALOR GLOBAL R$: Valor por extenso (_____)					

DECLARO, sob as sanções administrativas cabíveis, inclusive as criminais e sob as penas da lei, que toda documentação anexada ao sistema são autênticas.

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 20210007-ETICE
PROCESSO Nº 04358544/2021.

Aos __ dias do mês de _____ de 20__, na sede da Empresa de Tecnologia da Informação do Ceará - ETICE, foi lavrada a presente Ata de Registro de Preços, conforme deliberação da Ata do Pregão Eletrônico nº 20210007– ETICE do respectivo resultado homologado, publicado no Diário Oficial do Estado em __/__/20__, às fls ____, do Processo nº **04358544/2021**, que vai assinada pelo titular da Empresa de Tecnologia da Informação do Ceará – ETICE – gestora 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:

CLÁUSULA PRIMEIRA – DO FUNDAMENTO LEGAL

1.1. O presente instrumento fundamenta-se:

I. No Pregão Eletrônico nº 20210007– ETICE.
II. Nos termos do Decreto Estadual nº 32.824, de 11/10/2018, publicado D.O.E de 11/10/2018.
III. Na Lei Federal n.º 8.666, de 21.6.93 e nos Regulamento de Licitações e Contratos da ETICE

CLÁUSULA SEGUNDA - DO OBJETO

A presente Ata tem por objeto o Registro de preços para futuras e eventuais contratações 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 no Anexo I - Termo de Referência de Pregão Eletrônico nº 20210007- ETICE, que passa a fazer parte desta Ata, com as propostas de preços apresentadas pelos prestadores de serviços classificados em primeiro lugar, conforme consta nos autos do Processo nº **04358544/2021**.

Subcláusula Única - 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.

CLÁUSULA TERCEIRA - DA VALIDADE DA ATA DE REGISTRO DE PREÇOS

A presente Ata de Registro de Preços terá validade pelo prazo de 12 (doze) meses, contados a partir da data da sua publicação ou então até o esgotamento do quantitativo nela registrado, se este ocorrer primeiro.

CLÁUSULA QUARTA – DA GERÊNCIA DA ATA DE REGISTRO DE PREÇOS

Caberá a ETICE o gerenciamento deste instrumento, no seu aspecto operacional e nas questões legais, em conformidade com as normas do Decreto Estadual nº 32.824/2018, publicado no D.O.E de 11/10/2018.

CLÁUSULA QUINTA - DA UTILIZAÇÃO DA ATA DE REGISTRO DE PREÇOS

Em decorrência da publicação desta Ata, os órgãos/entidades participantes do SRP poderão firmar contratos com os prestadores de serviços com preços registrados, devendo comunicar ao órgão gestor, a recusa do detentor de registro de preços em executar os serviços no prazo estabelecido.

Subcláusula Primeira - O prestador de serviço 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. A critério da contratante, o contrato poderá ser assinado por certificação digital.

Subcláusula Segunda -Na assinatura do contrato, será exigida a comprovação das condições de habilitação exigidas no edital, as quais deverão ser mantidas pela contratada durante todo o período da contratação.

CLÁUSULA SEXTA - DAS OBRIGAÇÕES E RESPONSABILIDADES

Os signatários desta Ata de Registro de Preços assumem as obrigações e responsabilidades constantes no Decreto Estadual de Registro de Preços nº 32.824/2018.

Subcláusula Primeira - Competirá a ETICE na qualidade de gestor do Registro de Preços, o controle e administração do SRP, em especial, as atribuições estabelecidas nos incisos I ao VII, do art. 17, do Decreto Estadual n° 32.824/2018.

Subcláusula Segunda - Caberá aos órgão/entidades participantes, as atribuições que lhe são conferidas nos termos dos incisos I a V, do art. 18, do Decreto Estadual n° 32.824/2018.

Subcláusula Terceira - O detentor do registro de preços, durante o prazo de validade desta Ata, fica obrigado a:

a) atender aos pedidos efetuado(s) pelo(s) órgão(s) ou entidade(s) participante(s) do SRP, bem como aqueles decorrentes de remanejamento de quantitativos registrados nesta Ata, durante a sua vigência.

b) executar os serviços ofertados, por preço unitário registrado, nas quantidades indicadas pelos órgãos/entidades participantes do Sistema de Registro de Preços.

c) responder no prazo de até 5 (cinco) dias a consultas da ETICE, órgão gestor de Registro de Preços, sobre a pretensão de órgão(s)/entidade(s) não participantes.

d) Cumprir, quando for o caso, as condições de garantia do objeto, responsabilizando-se pelo período oferecido em sua proposta, observando o prazo mínimo exigido pela Administração.

CLÁUSULA SÉTIMA - DOS PREÇOS REGISTRADOS

Os preços registrados são os preços unitários ofertados nas propostas dos detentores de preços desta Ata, os quais estão relacionados no Mapa de Preços dos itens, anexo a este instrumento e servirão de base para futuras execuções de serviços, observadas as condições de mercado.

CLÁUSULA OITAVA – DA REVISÃO DOS PREÇOS REGISTRADOS

Os preços registrados só poderão ser revistos nos casos previstos no art. 23, do Decreto Estadual n° 32.824/2018.

CLÁUSULA NONA - DO CANCELAMENTO DO REGISTRO DE PREÇOS

Os preços registrados na presente Ata, poderão ser cancelados de pleno direito, nas situações previstas no art. 25, e na forma do art. 26, ambos do Decreto Estadual n° 32.824/2018.

CLÁUSULA DÉCIMA - DAS CONDIÇÕES PARA A EXECUÇÃO

Os serviços que poderão advir desta Ata de Registro de Preços serão formalizadas por meio de instrumento contratual a ser celebrado entre os órgão(s)/entidade(s) participante(s) e o prestador do serviço.

Subcláusula Primeira - Caso o prestador do serviço classificado em primeiro lugar, não cumpra o prazo estabelecido pelos órgãos/entidades participantes ou se recuse a executar o serviço, terá o seu registro de preço cancelado, sem prejuízo das demais sanções previstas em lei e nesta Ata.

Subcláusula Segunda - Neste caso, o órgão/entidade participante comunicará a ETICE órgão gestor, competindo a esta convocar sucessivamente por ordem de classificação, os demais prestadores de serviços.

CLÁUSULA DÉCIMA PRIMEIRA - DAS SANÇÕES ADMINISTRATIVAS

Subcláusula Primeira - O prestador de serviço que praticar quaisquer das condutas previstas nos incisos I, II, III, V, VIII, IX e X do art. 37, do Decreto Estadual nº 33.326/2019, sem prejuízo das sanções legais nas esferas civil e criminal, estará sujeito às seguintes penalidades:

a) Multa de 10% (dez por cento) sobre o preço total do (s) item (ns) registrado(s).

b) Impedimento de licitar e contratar com a Administração, sendo, então, descredenciado no cadastro de fornecedores da Secretaria do Planejamento e Gestão (SEPLAG), do Estado do Ceará, pelo prazo de até 5 (cinco) anos, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, sem prejuízo da multa prevista neste instrumento e das demais cominações legais.

Subcláusula Segunda – O prestador de serviço 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.

Subcláusula Terceira - A multa poderá ser aplicada com outras sanções segundo a natureza e a gravidade da falta cometida, desde que observado o princípio da proporcionalidade.

Subcláusula Quarta – Nenhuma sanção será aplicada sem garantia da ampla defesa e contraditório, na forma da lei.

CLÁUSULA DÉCIMA SEGUNDA – DAS DISPOSIÇÕES GERAIS

As condições gerais da contratação, tais como os prazos para entrega e recebimento do objeto, as obrigações da contratante e da contratada, condições de pagamento, penalidades e demais condições do ajuste, encontram-se definidos no Termo de Referência e na Minuta do Contrato.

CLÁUSULA DÉCIMA TERCEIRA - DO FORO

Fica eleito o foro do município de Fortaleza, do Estado do Ceará, 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 Gestor	Nome do Titular	Cargo	CPF	RG	Assinatura

Detentores do Registro de Preços	Nome do Representante	Cargo	CPF	RG	Assinatura

ANEXO ÚNICO DA ATA DE REGISTRO DE PREÇOS Nº ___ /20__ - MAPA DE PREÇOS DOS SERVIÇOS

Este documento é parte da Ata de Registro de Preços acima referenciada, celebrada entre a Empresa de Tecnologia da Informação do Ceará - ETICE e o Prestador de Serviço, cujos preços estão a seguir registrados por item, em face da realização do Pregão Eletrônico nº 20210007- ETICE.

ITEM	CÓD. DO ITEM	ESPECIFICAÇÃO DO ITEM	PRESTADORES DE SERVIÇO	QUANTIDADE	PREÇO REGISTRADO (R$)

ANEXO IV - MINUTA DO CONTRATO

CONTRATO Nº ____ / _____.
PROCESSO Nº 04358544/2021 - ETICE.

CONTRATO QUE ENTRE SI CELEBRAM A EMPRESA DE TECNOLOGIA DA INFORMAÇÃO DO CEARÁ - ETICE E (O) A _____, ABAIXO QUALIFICADOS, PARA O FIM QUE NELE SE DECLARA.

A EMPRESA DE TECNOLOGIA DA INFORMAÇÃO DO CEARÁ - ETICE, situada na _____, inscrita no CNPJ sob o nº _____, doravante denominada CONTRATANTE, neste ato representada 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 denominada CONTRATADA, representada 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 edital do Pregão Eletrônico n° 20210007- ETICE e seus anexos, o os preceitos do direito privado, a Lei Federal nº 8.666/93, e outras leis especiais necessárias 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 20210007- ETICE e seus Anexos, e à proposta da CONTRATADA, os quais constituem parte deste instrumento, independente de sua transcrição.

CLÁUSULA TERCEIRA - DO OBJETO

3.1. Constitui objeto deste contrato o serviço para contratações 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 no Anexo I - Termo de Referência do Edital do Pregão Eletrônico nº 20210007- ETICE e na proposta da CONTRATADA.

CLÁUSULA QUARTA - DO REGIME DE EXECUÇÃO

4.1. O objeto dar-se-á sob o regime de execução indireta: empreitada por preço unitário.

CLÁUSULA QUINTA – DOS PREÇOS E DO REAJUSTAMENTO

5.1. O preço contratual global importa na quantia de R$ _____(_____), sujeito a reajustes, desde que observado o interregno mínimo de 01 (um) ano, a contar da apresentação da proposta, conforme art. 40, XI da Lei nº 8.666/93, art. 37, XXI da Constituição Federal e art. 3º,§ 1º da Lei nº 10.192/2001.

5.1.1. Caso o prazo exceda a 01 (um) ano, o preço contratual será reajustado, utilizando a variação do índice nacional de preços ao Consumidor Amplo - **IPCA**, calculado pelo Instituto Brasileiro de Geografia e Estatística - IBGE.

CLÁUSULA SEXTA - DO PAGAMENTO

6.1.O pagamento advindo do objeto da Ata de Registro de Preços será proveniente dos recursos do (s) próprios órgão (s)/entidades participante (s) e será efetuado mensalmente até 30 (trinta) dias a contar da data da apresentação da Nota Fiscal/Fatura devidamente atestada pelo gestor da contratação, mediante crédito em conta corrente em nome da contratada, exclusivamente no Banco Bradesco S/A, conforme Lei nº 15.241, de 06 de dezembro de 2012, salvo as economias mistas e suas subsidiárias com exceção da Companhia de Água e Esgoto – CAGECE.

6.2 A nota fiscal/fatura que apresente incorreções será devolvida à contratada para as devidas correções. Nesse caso, o prazo de que trata o subitem anterior começará a fluir a partir da data de apresentação da nota fiscal/fatura corrigida.

6.3. No caso dos itens 26 a 29 o pagamento será realizado mensalmente referente a quantidade de itens que estão sendo monitorados e/ou mantidos.

6.4. Não será efetuado qualquer pagamento à CONTRATADA, antes da execução do objeto, se o objeto não estiver de acordo com as especificações deste instrumento e em caso de descumprimento das condições de habilitação exigidas na licitação.

6.5 No caso de atraso de pagamento, desde que a contratada não tenha concorrido de alguma forma para tanto, serão devidos pela contratante encargos moratórios à taxa nominal de 6% a.a. (seis por cento ao ano), capitalizados diariamente em regime de juros simples.

6.6. O valor dos encargos será calculado pela fórmula: EM = I x N x VP, onde: EM = Encargos moratórios devidos, N = Números de dias entre a data prevista para o pagamento e a do efetivo pagamento, I = Índice de compensação financeira = 0,00016438 e VP = Valor da prestação em atraso.
6.7. Os pagamentos encontram-se ainda condicionados à apresentação dos seguintes comprovantes:
6.8. Certidão Conjunta Negativa de Débitos relativos aos Tributos Federais e à Dívida Ativa da União, Certidão Negativa de Débitos Estaduais, Certidão Negativa de Débitos Municipais, Certificado de Regularidade do FGTS - CRF, Certidão Negativa de Débitos Trabalhistas – CNDT.
6.9. Toda a documentação exigida deverá ser apresentada em original ou por qualquer processo de reprografia, autenticada por cartório competente ou por servidor da Administração, ou publicação em órgão da imprensa oficial. Caso a documentação tenha sido emitida pela internet, só será aceita após a confirmação de sua autenticidade.

CLÁUSULA SÉTIMA - DOS RECURSOS ORÇAMENTÁRIOS

7.1. As despesas decorrentes da contratação serão provenientes dos recursos _____.

CLÁUSULA OITAVA – DO PRAZO DE VIGÊNCIA, DE EXECUÇÃO E DA ALTERAÇÃO DO CONTRATO

8.1 Os prazos de vigência e de execução contratual obedecerão ao disposto abaixo:
8.1.1.Em caso de contratação dos itens 1 a 25, os prazos de vigência e de execução contratual serão de 12 (doze) meses, contados a partir do recebimento da ordem de serviço.
8.1.2. Em caso de contratação dos itens 26 a 30, os prazos de vigência e de execução contratual serão de 36 (trinta e seis) meses, contados a partir do recebimento da ordem de serviço.
8.2. Os prazos de vigência e de execução poderão ser prorrogados nos termos do art. 57 da Lei Federal n° 8.666/1993.
8.3.. A publicação resumida do instrumento de contrato dar-se-á na forma do parágrafo único, do art. 61, da Lei Federal nº 8.666/1993

CLÁUSULA NONA - DA GARANTIA CONTRATUAL

9.1. A CONTRATADA deverá apresentar à Administração da CONTRATANTE, no prazo máximo de 10 (dez) dias úteis, contado da assinatura do respectivo instrumento, comprovante de prestação de garantia de 5% (cinco porcento) sobre o valor do contrato, em conformidade com o disposto no art. 56, da Lei Federal no 8.666/1993, vedada à prestação de garantia através de Título da Dívida Agrária.
9.2. A inobservância do prazo fixado para apresentação da garantia acarretará a aplicação de multa de 0,07% (sete centésimos por cento) do valor deste contrato por dia de atraso, até o máximo de 2% (dois por cento).
9.3. A garantia prestada, de acordo com o estipulado no edital, será restituída e/ou liberada após o cumprimento integral de todas as obrigações contratuais e, quando em dinheiro, será atualizada monetariamente, conforme dispõe o § 4º, do art. 56, da Lei Federal nº 8.666/1993. Na ocorrência de acréscimo contratual de valor, deverá ser prestada garantia proporcional ao valor acrescido, nas mesmas condições inicialmente estabelecidas.
9.4. A validade da garantia, qualquer que seja a modalidade escolhida, deverá abranger um período de 90 dias após o término da vigência contratual.
9.5. A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:
9.5.1. Prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;
9.5.2. Prejuízos diretos causados à Administração decorrentes de culpa ou dolo durante a execução do contrato.

CLÁUSULA DÉCIMA - DA ENTREGA E DO RECEBIMENTO

10.1. Quanto à entrega:

10.1.1. Os itens 1 a 20 deverão ser entregues em conformidade com as especificações estabelecidas neste instrumento, em um prazo máximo de 90 (noventa) dias úteis contados a partir do recebimento da ordem de serviço ou instrumento hábil.
10.1.2.O objeto contratual deverá ser entregue em conformidade com as especificações estabelecidas neste instrumento. O Local de entrega e os endereços específicos de cada localidade beneficiada serão repassados pela CONTRATANTE a CONTRATADA, de acordo com o estabelecido na Ordem de Serviço.
10.1.3. Os atrasos ocasionados por motivo de força maior ou caso fortuito, desde que justificados até 2 (dois) dias úteis antes do término do prazo de execução, e aceitos pela CONTRATANTE, não serão considerados como inadimplemento contratual.

10.2. Quanto ao recebimento:

10.2.1. PROVISORIAMENTE, mediante recibo, para efeito de posterior verificação da conformidade do objeto com as especificações, devendo ser feito por pessoa credenciada pela CONTRATANTE.
10.2.2.DEFINITIVAMENTE, sendo expedido termo de recebimento definitivo, após a verificação da qualidade e quantidade do objeto, certificando-se de que todas as condições estabelecidas foram atendidas e consequente aceitação das notas fiscais pelo gestor da contratação, devendo haver rejeição no caso de desconformidade.

CLÁUSULA DÉCIMA PRIMEIRA - DAS OBRIGAÇÕES DA CONTRATADA

11.1. Executar o objeto em conformidade com as condições deste instrumento.

11.2. Manter durante toda a execução contratual, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

11.3. Aceitar, nas mesmas condições contratuais, os percentuais de acréscimos ou supressões limitados ao estabelecido no §1º, do art. 65, da Lei Federal nº 8.666/1993, tomando-se por base o valor contratual.

11.4. Responsabilizar-se pelos danos causados diretamente à CONTRATANTE ou a terceiros, decorrentes da sua culpa ou dolo, quando da execução do objeto, não podendo ser arguido para efeito de exclusão ou redução de sua responsabilidade o fato da CONTRATANTE proceder à fiscalização ou acompanhar a execução contratual.

11.5. Responder por todas as despesas diretas e indiretas que incidam ou venham a incidir sobre a execução contratual, inclusive as obrigações relativas a salários, previdência social, impostos, encargos sociais e outras providências, respondendo obrigatoriamente pelo fiel cumprimento das leis trabalhistas e específicas de acidentes do trabalho e legislação correlata, aplicáveis ao pessoal empregado na execução contratual. A inadimplência da contratada quanto aos encargos trabalhistas, fiscais e comerciais não transfere à CONTRATANTE a responsabilidade por seu pagamento, nem poderá onerar o objeto do contrato.

11.6. Prestar imediatamente as informações e os esclarecimentos que venham a ser solicitados pela contratante, salvo quando implicarem em indagações de caráter técnico, hipótese em que serão respondidas no prazo de 24 (vinte e quatro) horas.

11.7. Refazer, substituir ou reparar o objeto contratual que comprovadamente apresente condições de defeito ou em desconformidade com as especificações deste termo, no prazo fixado pelo (s) órgão (s) /entidade (s) participante (s) do SRP (Sistema de Registro de Preços), contado da sua notificação.

11.8. Cumprir, quando for o caso, as condições de garantia do objeto, responsabilizando-se pelo período oferecido em sua proposta comercial, observando o prazo mínimo exigido pela Administração.

11.9. Providenciar a substituição de qualquer empregado que esteja a serviço da contratante, cuja conduta seja considerada indesejável pela fiscalização da contratante.

11.10. Responsabilizar-se integralmente pela observância do dispositivo no título II, capítulo V, da CLT, e na Portaria nº 3.460/77, do Ministério do Trabalho, relativos a segurança e higiene do trabalho, bem como a Legislação correlata em vigor a ser exigida.

11.11. Respeitar a legislação relativa à disposição final ambientalmente adequada dos resíduos gerados, mitigação dos danos ambientais por meio de medidas condicionantes e de compensação ambiental e outros, conforme previsto em lei.

11.12. Disponibilizar nos termos da Lei nº 15.854, de 24/09/2015, vagas de empregos a presos em regime semiaberto, aberto, em livramento condicional e egressos do sistema prisional e aos jovens do sistema socioeducativo entre 16 e 18 anos, que estejam cumprindo medida de semiliberdade. Caso a execução contratual não necessite, ou necessite de 5 (cinco) ou menos trabalhadores, a reserva de vagas será facultativa.

11.12.1.Encaminhar mensalmente, respectivamente, à CISPE/SEJUS e à SPS, a folha de frequência dos presos e egressos e/ou jovens do sistema socioeducativo, contemplados com a reserva de vagas. Caso a contratação não esteja obrigada a disponibilizar vagas nos termos da Lei nº 15.854, de 24/09/2015 ficará dispensada do envio da folha de frequência.

CLÁUSULA DÉCIMA SEGUNDA - DAS OBRIGAÇÕES DA CONTRATANTE

12.1. Solicitar a execução do objeto à contratada através da emissão de Ordem de Fornecimento/ Serviço.

12.2. Proporcionar à CONTRATADA todas as condições necessárias ao pleno cumprimento das obrigações decorrentes do objeto contratual, consoante estabelece a Lei Federal nº 8.666/1993 e suas alterações.

12.3. Fiscalizar a execução do objeto contratual, através de sua unidade competente, podendo, em decorrência, solicitar providências da contratada, que atenderá ou justificará de imediato.

12.4. Notificar a contratada de qualquer irregularidade decorrente da execução do objeto contratual.

12.5. Efetuar os pagamentos devidos à contratada nas condições estabelecidas neste Termo.

12.6. Aplicar as penalidades previstas em lei e neste instrumento.

CLÁUSULA DÉCIMA TERCEIRA - DA FISCALIZAÇÃO

13.1. A execução contratual será acompanhada e fiscalizada por um representante especialmente designado para este fim pela CONTRATANTE a ser informado quando da lavratura do instrumento contratual.

CLÁUSULA DÉCIMA QUARTA - DAS SANÇÕES ADMINISTRATIVAS

14.1. No caso de inadimplemento de suas obrigações, a CONTRATADA estará sujeita, sem prejuízo das sanções legais nas esferas civil e criminal, às seguintes penalidades:

14.1.1. Multas, estipuladas na forma a seguir:

a) Multa de 0,07% (sete centésimos por cento) do valor deste contrato, por dia de atraso, até o máximo de 2% (dois por cento) pela inobservância do prazo fixado para apresentação da garantia.

b. Multa diária de 0,3% (três décimos por cento), no caso de atraso na execução do objeto contratual até o 30º (trigésimo) dia, sobre o valor da nota de empenho ou instrumento equivalente.
c. Multa diária de 0,5% (cinco décimos por cento), no caso de atraso na execução do objeto contratual superior a 30 (trinta) dias, sobre o valor da nota de empenho ou instrumento equivalente, até o limite do percentual fixado na alínea "e", hipótese que pode resultar na rescisão da avença. A aplicação da presente multa exclui a aplicação da multa prevista na alínea anterior.
d. Multa diária de 0,1% (um décimo por cento) sobre o valor da nota de empenho ou instrumento equivalente, em caso de descumprimento das demais cláusulas contratuais, elevada para 0,3% (três décimos por cento) em caso de reincidência.
e. Multa de 20% (vinte por cento) sobre o valor deste contrato, no caso de desistência da execução do objeto ou rescisão contratual não motivada pela CONTRATANTE, inclusive o cancelamento do registro de preço.
14.1.2. Impedimento de licitar e contratar com a Administração, sendo então, descredenciada no cadastro de fornecedores da Secretaria do Planejamento e Gestão (SEPLAG), do Estado do Ceará, pelo prazo de até 5 (cinco) anos, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, sem prejuízo das multas previstas neste instrumento e das demais cominações legais.
14.2. Se não for possível o pagamento da multa por meio de descontos dos créditos existentes, a CONTRATADA recolherá a multa por meio de Documento de Arrecadação Estadual (DAE), podendo ser substituído por outro instrumento legal, em nome da CONTRATANTE, se não o fizer, será cobrado em processo de execução.
14.3. A multa poderá ser aplicada com outras sanções segundo a natureza e a gravidade da falta cometida, desde que observado o princípio da proporcionalidade.
14.4. Nenhuma sanção será aplicada sem garantia da ampla defesa e contraditório, na forma da lei.

CLÁUSULA DÉCIMA QUINTA - DA FRAUDE E DA CORRUPÇÃO

15.1. A contratada deve observar e fazer observar, por seus fornecedores e subcontratados, se admitida subcontratação, o mais alto padrão de ética durante todo o processo de licitação, de contratação e de execução do objeto contratual. Para os propósitos desta cláusula, definem-se as seguintes práticas:
a) "prática corrupta": oferecer, dar, receber ou solicitar, direta ou indiretamente, qualquer vantagem com o objetivo de influenciar a ação de servidor público no processo de licitação ou na execução de contrato.
b) "prática fraudulenta": a falsificação ou omissão dos fatos, com o objetivo de influenciar o processo de licitação ou de execução de contrato.
c) "prática conluiada": esquematizar ou estabelecer um acordo entre dois ou mais licitantes, com ou sem o conhecimento de representantes ou prepostos do órgão licitador, visando estabelecer preços em níveis artificiais e não-competitivos.
d) "prática coercitiva": causar dano ou ameaçar causar dano, direta ou indiretamente, às pessoas ou sua propriedade, visando influenciar sua participação em um processo licitatório ou afetar a execução do contrato.
e) "prática obstrutiva":
(1) Destruir, falsificar, alterar ou ocultar provas em inspeções ou fazer declarações falsas aos representantes do organismo financeiro multilateral, com o objetivo de impedir materialmente a apuração de alegações de prática prevista nesta cláusula.
(2) Atos cuja intenção seja impedir materialmente o exercício do direito de o organismo financeiro multilateral promover inspeção.
15.2. Na hipótese de financiamento, parcial ou integral, por organismo financeiro multilateral, mediante adiantamento ou reembolso, este organismo imporá sanção sobre uma empresa ou pessoa física, para a outorga de contratos financiados pelo organismo se, em qualquer momento, constatar o envolvimento da empresa, diretamente ou por meio de um agente, em práticas corruptas, fraudulentas, conluiadas, coercitivas ou obstrutivas ao participar da licitação ou da execução um contrato financiado pelo organismo.
15.3. Considerando os propósitos dos itens acima, o contratado deverá concordar e autorizar que, na hipótese de o contrato vir a ser financiado, em parte ou integralmente, por organismo financeiro multilateral, mediante adiantamento ou reembolso, permitirá que o organismo financeiro e/ou pessoas por ele formalmente indicadas possam inspecionar o local de execução do contrato e todos os documentos e registros relacionados à licitação e à execução do contrato.
15.4. A contratante, garantida a prévia defesa, aplicará as sanções administrativas pertinentes, previstas em Lei, se comprovar o envolvimento de representante da empresa ou da pessoa física contratada em práticas corruptas, fraudulentas, conluiadas ou coercitivas, no decorrer da licitação ou na execução do contrato financiado por organismo financeiro multilateral, sem prejuízo das demais medidas administrativas, criminais e cíveis.

CLÁUSULA DÉCIMA SEXTA - DA SUBCONTRATAÇÃO

16.1. Será admitida a subcontratação se previamente aprovada pela CONTRATANTE, se não constituir o escopo principal do objeto e seja restrita ao percentual máximo de 30% (trinta por cento) da contratação.

16.2. A subcontratação de que trata esta cláusula, não exclui as responsabilidades da CONTRATADA perante a CONTRATANTE quanto a qualidade do objeto contratado, não constituindo portanto qualquer vínculo contratual ou legal da CONTRATANTE com a subcontratada.

16.3. A empresa subcontratada deverá atender, em relação ao objeto da subcontratação, as exigências de qualificação técnica impostas a CONTRATADA.

CLÁUSULA DÉCIMA SÉTIMA - DA RESCISÃO CONTRATUAL

17.1. A inexecução total ou parcial deste contrato e a ocorrência de quaisquer dos motivos constantes no art. 78, da Lei Federal nº 8.666/1993 será causa para sua rescisão, na forma do art. 79, com as consequências previstas no art. 80, do mesmo diploma legal.

17.2. Este contrato poderá ser rescindido a qualquer tempo pela CONTRATANTE, mediante aviso prévio de no mínimo 30 (trinta) dias, nos casos das rescisões decorrentes do previsto no inciso XII, do art. 78, da Lei Federal nº 8.666/1993, sem que caiba à CONTRATADA direito à indenização de qualquer espécie.

CLÁUSULA DÉCIMA OITAVA - DO FORO

18.1. Fica eleito o foro do município de CONTRATANTE, capital do Estado do Ceará, para dirimir quaisquer questões decorrentes da execução deste contrato, que não puderem ser resolvidas na esfera administrativa.

E, por estarem de acordo, foi mandado lavrar o presente contrato, que está visado pela Assessoria Jurídica da 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(A)

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)

ANEXO V - MINUTA DO CONTRATO - ESTATAIS

Contrato nº ____ / _____
Processo nº 04358544/2021-ETICE

CONTRATO QUE ENTRE SI CELEBRAM O (A)_____ _____ E (O) A _____, ABAIXO QUALIFICADOS, PARA O FIM QUE NELE SE DECLARA.

O _____, situada na _____, inscrita no CNPJ sob o nº _____, doravante denominada CONTRATANTE, neste ato representada 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 denominada CONTRATADA, representada 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 edital do Pregão Eletrônico n° 20210007 e seus anexos, os preceitos do direito privado, a Lei Federal nº 13.303/2016 , Regulamento de Licitações e Contratos da CONTRATANTE e outras leis especiais necessárias 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 20210007 e seus Anexos, e à proposta da CONTRATADA, os quais constituem parte deste instrumento, independente de sua transcrição.

CLÁUSULA TERCEIRA – DO OBJETO

3.1. Constitui objeto deste contrato as contratações 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 no Anexo I - Termo de Referência do Edital do Pregão Eletrônico nº 20210007 e na proposta da CONTRATADA.

CLÁUSULA QUARTA – DO REGIME DE EXECUÇÃO

4.1. O objeto dar-se-á sob o regime de execução indireta: Empreitada por preço unitário.

CLÁUSULA QUINTA – DO VALOR E DO REAJUSTAMENTO DO PREÇO

5.1. O preço contratual global importa na quantia de R$ _____(_____), sujeito a reajustes, desde que observado o interregno mínimo de 01 (um) ano, a contar da apresentação da proposta, conforme art. 37, XXI da Constituição Federal e art. 3º,§ 1º da Lei nº 10.192/2001.

5.1.1. Caso o prazo exceda a 01 (um) ano, o preço contratual será reajustado, utilizando a variação do índice nacional de preços ao Consumidor Amplo – **IPCA**.

CLÁUSULA SEXTA – DO PAGAMENTO

6.1.O pagamento advindo do objeto da Ata de Registro de Preços será proveniente dos recursos do (s) próprios órgão (s)/entidades participante (s) e será efetuado mensalmente até 30 (trinta) dias a contar da data da apresentação da Nota Fiscal/Fatura devidamente atestada pelo gestor da contratação, mediante crédito em conta corrente em nome da contratada, exclusivamente no Banco Bradesco S/A, conforme Lei nº 15.241, de 06 de dezembro de 2012, salvo as economias mistas e suas subsidiárias com exceção da Companhia de Água e Esgoto – CAGECE.

6.2 A nota fiscal/fatura que apresente incorreções será devolvida à contratada para as devidas correções. Nesse caso, o prazo de que trata o subitem anterior começará a fluir a partir da data de apresentação da nota fiscal/fatura corrigida.

6.3. No caso dos itens 26 a 29 o pagamento será realizado mensalmente referente a quantidade de itens que estão sendo monitorados e/ou mantidos.

6.4. Não será efetuado qualquer pagamento à CONTRATADA, antes da execução do objeto, se o objeto não estiver de acordo com as especificações deste instrumento e em caso de descumprimento das condições de habilitação exigidas na licitação.

6.5 No caso de atraso de pagamento, desde que a contratada não tenha concorrido de alguma forma para tanto, serão devidos pela contratante encargos moratórios à taxa nominal de 6% a.a. (seis por cento ao ano), capitalizados diariamente em regime de juros simples.

6.6. O valor dos encargos será calculado pela fórmula: EM = I x N x VP, onde: EM = Encargos moratórios devidos, N = Números de dias entre a data prevista para o pagamento e a do efetivo pagamento, I = Índice de compensação financeira = 0,00016438 e VP = Valor da prestação em atraso.

6.7. Os pagamentos encontram-se ainda condicionados à apresentação dos seguintes comprovantes:

6.8. Certidão Conjunta Negativa de Débitos relativos aos Tributos Federais e à Dívida Ativa da União, Certidão Negativa de Débitos Estaduais, Certidão Negativa de Débitos Municipais, Certificado de Regularidade do FGTS - CRF, Certidão Negativa de Débitos Trabalhistas – CNDT.
6.9. Toda a documentação exigida deverá ser apresentada em original ou por qualquer processo de reprografia, autenticada por cartório competente ou por servidor da Administração, ou publicação em órgão da imprensa oficial. Caso a documentação tenha sido emitida pela internet, só será aceita após a confirmação de sua autenticidade.

CLÁUSULA SÉTIMA – DOS RECURSOS ORÇAMENTÁRIOS

7.1. As despesas decorrentes da contratação serão provenientes dos recursos _____.

CLÁUSULA OITAVA – DO PRAZO DE VIGÊNCIA E DE EXECUÇÃO

8.1. Os prazos de vigência e de execução contratual obedecerão ao disposto abaixo:
8.1.1. Em caso de contratação dos itens 1 a 25, os prazos de vigência e de execução contratual serão de 12 (doze) meses, contados a partir da celebração do contrato conforme disposto no art. 71 da Lei nº 13.303/2016 para as empresas públicas, economia mistas e suas subsidiárias
8.1.2. Em caso de contratação dos itens 26 a 30, os prazos de vigência e de execução contratual serão de 36 (trinta e seis) meses, contados a partir da celebração do contrato conforme disposto no art. 71 da Lei nº 13.303/2016 para as empresas públicas, economia mistas e suas subsidiárias.
8.2. Este contrato poderá ser prorrogado nos termos do art. 71 da Lei Federal nº 13.303/2016 e no Regulamento de Licitações e Contratos da CONTRATANTE.
8.3. A publicação resumida do contrato dar-se-á nos termos do § 2º do art. 51 da Lei nº 13.303/2016.

CLÁUSULA NONA – DA GARANTIA CONTRATUAL

9.1. A CONTRATADA deverá apresentar à Administração da CONTRATANTE, no prazo máximo de 10 (dez) dias úteis, contado da assinatura do respectivo instrumento, comprovante de prestação de garantia de 5% (cinco por cento) sobre o valor do contrato, em conformidade com o disposto no art. 70, da Lei Federal nº 13.303/2016, vedada à prestação de garantia através de Título da Dívida Agrária.

9.2. A inobservância do prazo fixado para apresentação da garantia acarretará a aplicação de multa de 0,07% (sete centésimos por cento) do valor do contrato por dia de atraso, até o máximo de 2% (dois por cento).

9.3. A garantia prestada, de acordo com o estipulado no edital, será restituída e/ou liberada após o cumprimento integral de todas as obrigações contratuais e, quando em dinheiro, será atualizada monetariamente, conforme dispõe o § 4º, do art. 70, da Lei Federal nº 13.303/20176. Na ocorrência de acréscimo contratual de valor, deverá ser prestada garantia proporcional ao valor acrescido, nas mesmas condições inicialmente estabelecidas.

9.4. A validade da garantia, qualquer que seja a modalidade escolhida, deverá abranger um período de 90 dias após o término da vigência contratual.

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

9.5.1. Prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;

9.5.2. Prejuízos diretos causados à Administração decorrentes de culpa ou dolo durante a execução do contrato.

CLÁUSULA DÉCIMA – DA ENTREGA E DO RECEBIMENTO

10.1. Quanto à entrega:

10.1.1. Os itens 1 a 20 deverão ser entregues em conformidade com as especificações estabelecidas neste instrumento, em um prazo máximo de 90 (noventa) dias úteis contados a partir do recebimento da ordem de serviço ou instrumento hábil.
10.1.2.O objeto contratual deverá ser entregue em conformidade com as especificações estabelecidas neste instrumento. O Local de entrega e os endereços específicos de cada localidade beneficiada serão repassados pela CONTRATANTE a CONTRATADA, de acordo com o estabelecido na Ordem de Serviço.
10.1.3. Os atrasos ocasionados por motivo de força maior ou caso fortuito, desde que justificados até 2 (dois) dias úteis antes do término do prazo de execução, e aceitos pela CONTRATANTE, não serão considerados como inadimplemento contratual.

10.2. Quanto ao recebimento:

10.2.1. PROVISORIAMENTE, mediante recibo, para efeito de posterior verificação da conformidade do objeto com as especificações, devendo ser feito por pessoa credenciada pela CONTRATANTE.

10.2.2.DEFINITIVAMENTE, sendo expedido termo de recebimento definitivo, após a verificação da qualidade e quantidade do objeto, certificando-se de que todas as condições estabelecidas foram atendidas e consequente aceitação das notas fiscais pelo gestor da contratação, devendo haver rejeição no caso de desconformidade.

CLÁUSULA DÉCIMA PRIMEIRA – DAS OBRIGAÇÕES DA CONTRATADA

11.1. Executar o objeto em conformidade com as condições deste instrumento.

11.2. Manter durante toda a execução contratual, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação.
11.3. Refazer o objeto do contrato em que se verificarem vícios, defeitos ou incorreções resultantes da execução, bem como em desconformidade com as especificações do Anexo I - Termo de Referência ou de materiais empregados, e responderá por danos causados diretamente a terceiros ou à CONTRATANTE, independentemente da comprovação de sua culpa ou dolo na execução do contrato, não podendo ser arguido para efeito de exclusão ou redução de sua responsabilidade o fato de a CONTRATANTE proceder à fiscalização ou acompanhar a execução contratual.
11.3.1. Para cumprimento do previsto neste subitem, será concedido o prazo de 90 (noventa) dias, contado da notificação.
11.5. Responder por todas as despesas diretas e indiretas que incidam ou venham a incidir sobre a execução contratual, inclusive as obrigações relativas a salários, previdência social, impostos, encargos sociais e outras providências, respondendo obrigatoriamente pelo fiel cumprimento das leis trabalhistas e específicas de acidentes do trabalho e legislação correlata, aplicáveis ao pessoal empregado na execução contratual. A inadimplência da contratada quanto aos encargos trabalhistas, fiscais e comerciais não transfere à CONTRATANTE a responsabilidade por seu pagamento, nem poderá onerar o objeto do contrato.
11.6. Prestar imediatamente as informações e os esclarecimentos que venham a ser solicitados pela contratante, salvo quando implicarem em indagações de caráter técnico, hipótese em que serão respondidas no prazo de 24 (vinte e quatro) horas.
11.7. Cumprir, quando for o caso, as condições de garantia do objeto, responsabilizando-se pelo período oferecido em sua proposta comercial, observando o prazo mínimo exigido pela Administração.
11.8. Providenciar a substituição de qualquer empregado que esteja a serviço da contratante, cuja conduta seja considerada indesejável pela fiscalização da contratante.
11.9. Responsabilizar-se integralmente pela observância do dispositivo no título II, capítulo V, da CLT, e na Portaria nº 3.460/77, do Ministério do Trabalho, relativos a segurança e higiene do trabalho, bem como a Legislação correlata em vigor a ser exigida.
11.10. Respeitar a legislação relativa à disposição final ambientalmente adequada dos resíduos gerados, mitigação dos danos ambientais por meio de medidas condicionantes e de compensação ambiental e outros, conforme previsto em lei.
11.11. Disponibilizar nos termos da Lei nº 15.854, de 24/09/2015, vagas de empregos a presos em regime semiaberto, aberto, em livramento condicional e egressos do sistema prisional e aos jovens do sistema socioeducativo entre 16 e 18 anos, que estejam cumprindo medida de semiliberdade. Caso a execução contratual não necessite, ou necessite de 5 (cinco) ou menos trabalhadores, a reserva de vagas será facultativa.
11.11.1.Encaminhar mensalmente, respectivamente, à CISPE/SEJUS e à SPS, a folha de frequência dos presos e egressos e/ou jovens do sistema socioeducativo, contemplados com a reserva de vagas. Caso a contratação não esteja obrigada a disponibilizar vagas nos termos da Lei nº 15.854, de 24/09/2015 ficará dispensada do envio da folha de frequência.

CLÁUSULA DÉCIMA SEGUNDA– DAS OBRIGAÇÕES DA CONTRATANTE
12.1. Solicitar a execução do objeto à contratada através da emissão de Ordem de Fornecimento/ Serviço.
12.2. Proporcionar à CONTRATADA todas as condições necessárias ao pleno cumprimento das obrigações decorrentes do objeto contratual, consoante estabelece a Lei Federal nº 13.303/2016.
12.3. Fiscalizar a execução do objeto contratual, através de sua unidade competente, podendo, em decorrência, solicitar providências da contratada, que atenderá ou justificará de imediato.
12.4. Notificar a contratada de qualquer irregularidade decorrente da execução do objeto contratual.
12.5. Efetuar os pagamentos devidos à contratada nas condições estabelecidas neste Termo.
12.6. Aplicar as penalidades previstas em lei e neste instrumento.

CLÁUSULA DÉCIMA TERCEIRA – DA FISCALIZAÇÃO

13.1. A execução contratual será acompanhada e fiscalizada por um representante especialmente designado para este fim pela CONTRATANTE a ser informado quando da lavratura do instrumento contratual.

CLÁUSULA DÉCIMA QUARTA – DAS SANÇÕES ADMINISTRATIVAS
14.1. Pela inexecução total ou parcial do contrato, a contratante poderá, garantida a prévia defesa e o contraditório, aplicar a contratada, nos termos do art. 83 da Lei nº 13.303/2016 e dos arts. 166 a 169 do Regulamento de Licitações e Contratos da ETICE, as seguintes penalidades:
14.1.1. Advertência
14.1.2. Multas, estipuladas na forma a seguir:
a) Multa de 0,07% (sete centésimos por cento) do valor deste contrato, por dia de atraso, até o máximo de 2% (dois por cento) pela inobservância do prazo fixado para apresentação da garantia.
b. Multa diária de 0,3% (três décimos por cento), no caso de atraso na execução do objeto contratual até o 30º (trigésimo) dia, sobre o valor da nota de empenho ou instrumento equivalente.

c. Multa diária de 0,5% (cinco décimos por cento), no caso de atraso na execução do objeto contratual superior a 30 (trinta) dias, sobre o valor da nota de empenho ou instrumento equivalente, até o limite do percentual fixado na alínea "e", hipótese que pode resultar na rescisão da avença. A aplicação da presente multa exclui a aplicação da multa prevista na alínea anterior.

d. Multa diária de 0,1% (um décimo por cento) sobre o valor da nota de empenho ou instrumento equivalente, em caso de descumprimento das demais cláusulas contratuais, elevada para 0,3% (três décimos por cento) em caso de reincidência.

e. Multa de 20% (vinte por cento) sobre o valor deste contrato, no caso de desistência da execução do objeto ou rescisão contratual não motivada pela CONTRATANTE, inclusive o cancelamento do registro de preço.

14.1.3. Suspensão temporária de participação em licitação e impedimento de contratar com a entidade sancionadora, por prazo não superior a 2 (dois) anos.

14.2. Se não for possível o pagamento da multa por meio de descontos dos créditos existentes, a CONTRATADA recolherá a multa por meio de depósito bancário em nome da CONTRATANTE, se não o fizer, será cobrada em processo de execução.

14.3. A multa poderá ser aplicada com outras sanções segundo a natureza e a gravidade da falta cometida, desde que observado o princípio da proporcionalidade.

14.4. Nenhuma sanção será aplicada sem garantia da ampla defesa e contraditório, na forma da lei.

CLÁUSULA DÉCIMA QUINTA – DA FRAUDE E DA CORRUPÇÃO

15.1. A contratada deve observar e fazer observar, por seus fornecedores e subcontratados, se admitida subcontratação, o mais alto padrão de ética durante todo o processo de licitação, de contratação e de execução do objeto contratual. Para os propósitos desta cláusula, definem-se as seguintes práticas:

a) "prática corrupta": oferecer, dar, receber ou solicitar, direta ou indiretamente, qualquer vantagem com o objetivo de influenciar a ação de servidor público no processo de licitação ou na execução de contrato;

b) "prática fraudulenta": a falsificação ou omissão dos fatos, com o objetivo de influenciar o processo de licitação ou de execução de contrato;

c) "prática conluiada": esquematizar ou estabelecer um acordo entre dois ou mais licitantes, com ou sem o conhecimento de representantes ou prepostos do órgão licitador, visando estabelecer preços em níveis artificiais e não-competitivos;

d) "prática coercitiva": causar dano ou ameaçar causar dano, direta ou indiretamente, às pessoas ou sua propriedade, visando influenciar sua participação em um processo licitatório ou afetar a execução do contrato.

e) "prática obstrutiva":

(1) destruir, falsificar, alterar ou ocultar provas em inspeções ou fazer declarações falsas aos representantes do organismo financeiro multilateral, com o objetivo de impedir materialmente a apuração de alegações de prática prevista nesta cláusula;

(2) atos cuja intenção seja impedir materialmente o exercício do direito de o organismo financeiro multilateral promover inspeção.

15.2. Na hipótese de financiamento, parcial ou integral, por organismo financeiro multilateral, mediante adiantamento ou reembolso, este organismo imporá sanção sobre uma empresa ou pessoa física, para a outorga de contratos financiados pelo organismo se, em qualquer momento, constatar o envolvimento da empresa, diretamente ou por meio de um agente, em práticas corruptas, fraudulentas, conluiadas, coercitivas ou obstrutivas ao participar da licitação ou da execução um contrato financiado pelo organismo.

15.3. Considerando os propósitos dos itens acima, o contratado deverá concordar e autorizar que, na hipótese de o contrato vir a ser financiado, em parte ou integralmente, por organismo financeiro multilateral, mediante adiantamento ou reembolso, permitirá que o organismo financeiro e/ou pessoas por ele formalmente indicadas possam inspecionar o local de execução do contrato e todos os documentos e registros relacionados à licitação e à execução do contrato.

15.4. A contratante, garantida a prévia defesa, aplicará as sanções administrativas pertinentes, previstas em Lei, se comprovar o envolvimento de representante da empresa ou da pessoa física contratada em práticas corruptas, fraudulentas, conluiadas ou coercitivas, no decorrer da licitação ou na execução do contrato financiado por organismo financeiro multilateral, sem prejuízo das demais medidas administrativas, criminais e cíveis.

CLÁUSULA DÉCIMA SEXTA – DA SUBCONTRATAÇÃO

16.1. Será admitida a subcontratação conforme disposto no art. 78 da Lei nº 13.303/2016 se previamente aprovada pela CONTRATANTE, se não constituir o escopo principal do objeto e seja restrita ao percentual máximo de 30% (trinta por cento) da contratação.

16.2. A subcontratação de que trata esta cláusula, não exclui as responsabilidades da CONTRATADA perante a CONTRATANTE quanto a qualidade do objeto contratado, não constituindo portanto qualquer vínculo contratual ou legal da CONTRATANTE com a subcontratada.

16.3. A empresa subcontratada deverá atender, em relação ao objeto da subcontratação, as exigências de qualificação técnica impostas a CONTRATADA.
16.4. É vedada a subcontratação de empresa ou consórcio que tenha participado:
16.4.1. Do procedimento licitatório do qual se originou a contratação.
16.4.2. Direta ou indiretamente, da elaboração de projeto básico ou executivo.

CLÁUSULA DÉCIMA SÉTIMA – DA RESCISÃO CONTRATUAL

17.1. A inexecução total ou parcial deste contrato será causa para sua rescisão, em cumprimento ao inciso VII do art. 69 da Lei Federal nº 13.303/16 e regulamento interno de licitações e Contratos da CONTRATANTE.

17.2. Este contrato poderá ser rescindido a qualquer tempo pela CONTRATANTE, mediante aviso prévio de no mínimo 30 (trinta) dias, nos casos das rescisões decorrentes de razões de interesse público de alta relevância e amplo conhecimento desde que justificado, sem que caiba à CONTRATADA direito à indenização de qualquer espécie.

CLÁUSULA DÉCIMA OITAVA – DO FORO

18.1. Fica eleito o foro do município de Fortaleza, Capital do Estado do Ceará, para dirimir quaisquer questões decorrentes da execução deste contrato, que não puderem ser resolvidas na esfera administrativa.

E, por estarem de acordo, foi mandado lavrar o presente contrato, que está visado pela Assessoria Jurídica da 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(A)

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)

ANEXO VI - MODELO DE DECLARAÇÃO DE AUTENTICIDADE DOS DOCUMENTOS

(PAPEL TIMBRADO DO PROPONENTE)

DECLARAÇÃO

(nome /razão social) _____, inscrita no CNPJ nº_____,por intermédio de seu representante legal o(a) Sr(a)_____, portador(a) da Carteira de Identidade nº_____e CPF nº _____, DECLARA, sob as sanções administrativas cabíveis, inclusive as criminais e sob as penas da lei, que toda documentação anexada ao sistema são autênticas.

Local e data

Assinatura do representante legal
(Nome e cargo)