PREGÃO ELETRÔNICO Nº 20190013 - ETICE/DITEC

PROCESSO Nº 10314312/2019

UASG: 943001

NÚMERO COMPRASNET: 1632 2019

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, nº 33.326, de 29 de outubro de 2019, nº 32.718, de 15 de junho de 2018, 32.824 de 11 de outubro de 2018, e subsidiariamente a Lei Federal nº. 8.666, de 21 de junho de 1993, com suas alterações, Lei Federal nº 13.303, de 30 de junho de 2016 e do disposto no presente edital e seus anexos. Havendo conflito entre as disposições da Lei Federal nº 8.666/93 e a Lei Federal nº 13.303/2016, predominarão as disposições da Lei Federal nº 8.666/93.

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 com 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 www.comprasnet.gov.br.

5.2. O certame será realizado por meio do sistema Comprasnet, no endereço eletrônico www.comprasnet.gov.br, pelo pregoeiro VINÍCIUS VINEIMAR RODRIGUES FERREIRA, telefone: (85)3459-6560.

6. DAS DATAS E HORÁRIOS DO CERTAME

6.1. INÍCIO DO ACOLHIMENTO DAS PROPOSTAS:_____/_____/20___.

6.2. DATA DE ABERTURA DAS PROPOSTAS: _____/_____/20___, às _____.

6.3. INÍCIO DA SESSÃO DE DISPUTA DE PREÇOS:_____/_____/20___, às _____.

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 do(s) órgão(s)/entidade(s) participante(s) do SRP (Sistema de Registro de Preços), a ser informada 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 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. Impedidas de licitar e contratar com a Administração.

9.4.3. Cujo administrador ou sócio detentor de mais de 5% (cinco por cento) do capital social seja diretor ou empregado da ETICE.

9.4.4. Suspensas temporariamente de participar de licitação e impedidas de contratar com a Administração.

9.4.5. Declaradas inidôneas pela Administração Pública, enquanto perdurarem os motivos determinantes desta condição.

9.4.6. Servidor público ou empresas cujos dirigentes, gerentes, sócios ou componentes de seu quadro sejam funcionários ou empregados públicos da entidade contratante ou responsável pela licitação.

9.4.7. Estrangeiras não autorizadas a comercializar no país.

9.4.8. Cujo estatuto ou contrato social, não inclua no objetivo social da empresa, atividade compatível com o objeto do certame.

9.4.9. Constituída por sócio de empresa que estiver suspensa, impedida ou declarada inidônea.

9.4.10. Cujo administrador seja sócio de empresa suspensa, impedida ou declarada inidônea.

9.4.11. 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.

9.4.12. Cujo administrador tenha sido sócio ou administrador de empresa suspensa, impedida ou declarada inidônea, no período dos fatos que deram ensejo à sanção.

9.4.13. Que tiver, nos seus quadros de diretoria, pessoa que participou, em razão de vínculo de mesma natureza, de empresa declarada inidônea.

9.4.14. Empregado ou dirigente da ETICE, como pessoa física.

9.4.15. Sob a forma de consórcio, qualquer que seja sua constituição.

9.4.16. Quem tenha relação de parentesco, até o terceiro grau civil, com:

9.4.16.1. Dirigente ou empregado da ETICE, neste último caso quando as atribuições do empregado envolvam a atuação na área responsável pela licitação ou contratação.

9.4.16.2. Autoridade do ente público a que a ETICE esteja vinculada.

9.4.17. 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.

9.4.18. 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.

9.4.19. As justificativas para a vedação da participação de Consórcios estão a seguir descritas.

9.4.19.1. 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”.

9.4.19.2. 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 litado 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.

9.4.19.3. 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.

9.4.19.4. 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.

9.4.19.5. 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.

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. Não serão conhecidas as impugnações apresentadas fora do prazo legal e/ou subscritas por representante não habilitado legalmente. A petição de impugnação deverá constar o endereço, e-mail e telefone do impugnante ou de seu representante legal.

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 que tratam os subitens 11.3. e 11.4. deste edital.

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 7 de julho de 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:

15.5.3.1. 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.

15.5.3.2. Atestado de capacidade técnica, fornecido por pessoa jurídica de direito público ou privado, que comprove que a licitante forneceu no mínimo 10 (dez) equipamentos do tipo Next Generation Firewall sob a forma de serviço gerenciado, incluindo suporte e monitoramento da solução.

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.v.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**

11.5.7.1. 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. 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.

11.6.1. 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” do subitem 11.6. deste edital.

11.7. 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

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 V – Declaração de autenticidade da documentação deste edital.

12.1.1. Constatada a ausência da declaração de autenticidade da documentação, não implicará no afastamento imediato da arrematante por considerar-se falha formal passível de saneamento nos termos do subitem 22.2. deste edital.

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, inclusive o cálculo da diferença entre o imposto(ICMS) devido à unidade federada de destino e a unidade federada de origem, conforme Emenda Constitucional nº 87/2015, para os itens 11 ao 13 e 17 a 23. O Campo “descrição detalhada do objeto ofertado” deverá ser preenchido.

12.2.1. 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, quantitativos, marca/modelo, nos termos do Anexo I - Termo de Referência deste edital.

12.2.2. Prazo de validade não inferior a 90 (noventa) dias, contados a partir da data da sua emissão.

12.2.3. Para efeito de julgamento das propostas eletrônicas referentes aos itens 11 ao 13 e 17 a 23, o valor a ser informado no sistema eletrônico, pelas licitantes situadas no Estado do Ceará, será o valor deduzido do percentual de 7,5% (sete inteiros e cinco décimos por cento), correspondente à média das diferenças de alíquotas interestaduais do ICMS, nos termos do disposto no Decreto Estadual nº 27.624/2004.

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

12.3. Para os itens de 01 a 10, no valor unitário deve ser informado o valor mensal do serviço, multiplicado por 12 (doze) meses.

12.4. As licitantes poderão retirar ou substituir as propostas e os documentos de habilitação por eles apresentados, até o término do prazo para recebimento.

12.5**.** Somente serão aceitas a realização de cotações, por fornecedor, que representem 100% (cem por cento) das quantidades demandadas.

12.6. 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.

12.7. 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.

12.8. Os documentos de habilitação deverão ser apresentados da seguinte forma:

12.8.1. 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.

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

12.8.3. 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.

12.8.3.1. Documentos de procedência estrangeira, emitidos em língua portuguesa, também deverão ser apresentados consularizados ou registrados em cartório de títulos e documentos.

12.8.4. 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. Não havendo vencedora para a cota reservada, esta poderá ser adjudicada a vencedora da cota principal, ou diante de sua recusa, as licitantes remanescentes, desde que pratiquem preço da primeira colocada.

15.4. 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.

15.4.1. A proposta deverá ser anexada em conformidade com o item 12.2. deste edital.

15.5. Encerrada a análise quanto à aceitação da proposta, o pregoeiro verificará a habilitação da licitante, observado o disposto neste Edital.

15.7. 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.

15.5. 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.

15.6. Nos termos do Decreto Estadual nº 27.624/2004, a arrematante dos itens de 11 ao 13 e 17 ao 23, situada no Estado do Ceará deverá apresentar a proposta com o valor acrescido do diferencial referido no subitem 12.2.3, mediante a utilização da seguinte fórmula;

$$VFP = \frac{VPV}{0,925}$$

Onde:

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

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

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

15.7. Para efeito de cálculo será observado o previsto no subitem 12.2 deste edital.

15.8. O licitante deverá fornecer junto com a proposta de preços:

15.8.1. Descrição detalhada das características técnicas dos itens cotados, que possibilitem uma completa avaliação dos mesmos. A licitante deverá fornecer uma matriz ponto a ponto comprovando cada item do edital, com a indicação da página do datasheet, manuais, certificação dos equipamentos e serviços que serão ofertados. A matriz de características técnicas é de preenchimento obrigatório pelo Licitante, sendo motivo de desclassificação do certame o seu não preenchimento.

15.8.2. O preenchimento da matriz de características técnicas deverá ser realizado baseado em documentos cuja origem seja exclusivamente do fabricante dos equipamentos, como catálogos, ou manuais, ou ficha de especificação técnica, ou 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. Serão aceitos documentos em português ou inglês para comprovações técnicas. A não comprovação de alguma característica exigida no Termo de Referência levará à desclassificação da proposta.

15.8.3. Comprovação das especificações técnicas como folder, manuais e catálogos.

15.8.4. Uma cópia em mídia (pendrive, cd, dvd, usb ou link no site do licitante) da documentação referente ao item 15.8.1.

15.9. 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**, observado o estabelecido no Decreto Estadual nº 27.624/2004 e 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 for aceitável, 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.

16.4.4. Se encontrem acima do orçamento estimado para a contratação após encerrada a negociação de menor preço.

16.4.5. Não tenham sua exequibilidade demonstrada, quando exigido pela ETICE.

16.4.6. Apresentem desconformidade com outras exigências do instrumento convocatório, salvo se for possível a acomodação a seus termos antes da adjudicação do objeto e sem que se prejudique a atribuição de tratamento isonômico entre as licitantes.

16.4.7. A ETICE poderá realizar diligências para aferir a exequibilidade das propostas ou exigir das licitantes que ela seja demonstrada.

16.4.8. Em condições ilegais, omissões, ou conflitos com as exigências deste edital.

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, de forma imediata, depois de aceito e habilitado, quando lhe será concedido o prazo de 3 (três) dias para apresentação das razões do recurso no sistema Comprasnet. As demais licitantes

ficam desde logo convidados 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 autos.

17.1.1. Para abertura do prazo recursal, 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, 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 o gestor a fim de assinarem a Ata de Registro de Preços, sob pena de decair do direito à contratação, e sem prejuízo das sanções previstas no Edital, podendo o prazo de comparecimento ser prorrogado uma vez, por igual período, desde que ocorra motivo justificado e aceito pela administração.

18.4. A Ata de Registro de Preços poderá ser assinada por certificação digital.

18.5. Homologada a licitação e obedecida a 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 facultado à Administração após a homologação da licitação e desde que, obedecida a 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 esta 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 o 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, 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 no art. 37, do Decreto Estadual nº 33.326/2019, sem prejuízo das sanções legais nas esferas civil e criminal, inclusive as decorrentes da Lei nº 12.846/2013, 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 ETICE dará publicidade da sanção administrativa para registro no Cadastro de Fornecedores do Estado.

19.3. A licitante recolherá a multa por meio de depósito bancário em nome da ETICE, Se não o fizer, será cobrada em processo de execução.

19.4. 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 da 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, será assinada pelo titular da Empresa da 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 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. A Empresa da Tecnologia da Informação do Ceará – ETICE, na condição de único participante do SRP (Sistema de Registro de Preços) quando necessitar, efetuará os serviços junto aos prestadores de serviços detentores de preços registrados na Ata de Registro de Preços, de acordo com as especificações e quantitativos previstos, durante a vigência do documento supracitado.

20.6. Os prestadores de serviços detentores de preços registrados ficarão obrigados a executar o objeto licitado ao participante 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 órgão ou entidade de outros entes federativos, como órgão interessado, mediante consulta prévia ao 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 ao órgão gestor do Registro de Preços, o qual indicará o prestador de serviço 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, independente do número de órgãos interessados que aderirem.

20.8.3. O órgão interessado deverá efetivar a aquisição ou contratação solicitada em até noventa dias, contados a partir da autorização do órgão gestor do registro de preços, observado o prazo de vigência da ata.

20.8.4. A comunicação ao 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 aquisição ou contratação.

20.8.5. O órgão gestor do registro de preços não autorizará a adesão à ata de registro de preços para contratação separada de itens de objeto adjudicado por preço global para os quais o fornecedor não tenha apresentado o menor preço.

20.9. Caberá ao órgão gestor do Registro de Preços, para utilização da Ata por órgãos interessados da Administração Pública, proceder a indicação do prestador de serviço detentor do preço registrado, obedecida a 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 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 ETICE convocará o prestador 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 prestador de serviço será liberado do compromisso assumido.

20.13. Não havendo êxito nas negociações com os prestadores de serviços com preços registrados, o 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 dos preços registrados, oriundas de revisão dos mesmos, serão publicadas no Diário Oficial do Estado e na página oficial do Governo do Estado na internet.

20.16. As demais condições contratuais se encontram estabelecidas no Anexo IV- Minuta do Contrato.

20.17. Os serviços previstos no Anexo I – Termo de Referência deste edital, são estimativas máximas para o período de validade da Ata de Registro de Preços, reservando-se a Administração, através do órgão participante, o direito de executá-los no quantitativo que julgar necessário ou mesmo abster-se do executar o item especificado.

20.18. DA GARANTIA CONTRATUAL

20.18.1. Após a homologação do objeto do certame e até a data da contratação, a licitante vencedora deverá prestar garantia contratual correspondente a 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.

20.18.2. Na garantia deverá estar expresso prazo de validade superior a 90 (noventa) dias do prazo contratual.

20.18.3. A não prestação de garantia equivale à recusa injustificada para a contratação, caracterizando descumprimento total da obrigação assumida, ficando a licitante sujeito às penalidades legalmente estabelecidas, inclusive multa.

20.19. DA SUBCONTRATAÇÃO

20.19.1. Será admitida a subcontratação no limite de 30% (trinta por cento) do objeto, conforme disposto no art. 78 da Lei nº 13.303/2016, desde que não constitua o escopo principal da contratação, e, se previamente aprovada pela ETICE.

20.19.2. A subcontratação de que trata esta cláusula, não exclui a responsabilidade da contratada perante a ETICE quanto à qualidade do objeto contratado, não constituindo portanto qualquer vínculo contratual ou legal da ETICE com a subcontratada.

20.19.3. A contratada ao requerer autorização para subcontratação de parte do objeto, deverá comprovar perante a Administração a regularidade jurídico/fiscal e trabalhista de sua subcontratada.

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 superior, 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. Os documentos referentes aos orçamentos, bem como o valor estimado da contratação, possuem caráter sigiloso e serão disponibilizados exclusivamente aos órgãos de controle interno e externo, conforme o disposto no art. 15 do Decreto Estadual n° 33.326/2019.

22.13. 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, 8 de janeiro de 2020.

_____ CIENTE: _____

Raimundo Osman Lima
PRESIDENTE DA ETICE EM EXERCÍCIO

Vinícius Vineimar Rodrigues Ferreira
PREGOEIRO

Aprovado:_____

(aprovação da assessoria ou procuradoria jurídica conforme o caso)

ANEXO I - TERMO DE REFERÊNCIA

1. UNIDADE REQUISITANTE: *ETICE / DITEC*

1. 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 com 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.

2. DA JUSTIFICATIVA:

3.1. As justificativas das necessidades das possíveis contratações de serviços 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. DAS ESPECIFICAÇÕES E QUANTITATIVOS

GRUPO ÚNICO: SOLUÇÃO DE PROTEÇÃO DE REDE SERVIÇOS E AQUISIÇÕES

TABELA DE SERVIÇOS

Item	Especificação	UNIDADE DE FORNEC.	Qtde
1	Firewall – CENTRAL TIPO I	unidade	10
2	Firewall – CENTRAL TIPO II	unidade	10
3	Firewall – CENTRAL TIPO III	unidade	8
4	Firewall – CENTRAL TIPO IV	unidade	4
5	Firewall – DATA CENTER TIPO I	unidade	4
6	Firewall – DATA CENTER TIPO II	unidade	4
7	Firewall – DATA CENTER TIPO III	unidade	2
8	Firewall para Nuvem Privada	unidade	20
9	Firewall para Nuvem Pública	unidade	25
10	Solução de Segurança e Visibilidade para Ambientes Multi-Cloud	unidade	2

TABELA DE AQUISIÇÃO

Item	Especificação	UNIDADE DE FORNEC.	Qtde
11	Firewall – UNIDADE REMOTA TIPO I	unidade	1200
12	Firewall – UNIDADE REMOTA TIPO II	unidade	100
13	Firewall – UNIDADE REMOTA TIPO III	unidade	25
14	Instalação e Configuração de Firewall até 100 KM de Fortaleza	unidade	1000

15	Instalação e Configuração de Firewall até 400 KM de Fortaleza	unidade	200
16	Instalação e Configuração de Firewall acima 400 KM de Fortaleza	unidade	200
17	Firewall – CENTRAL TIPO I - AQUISIÇÃO	unidade	1
18	Firewall – CENTRAL TIPO II – AQUISIÇÃO	unidade	1
19	Firewall – CENTRAL TIPO III – AQUISIÇÃO	unidade	1
20	Firewall – CENTRAL TIPO IV – AQUISIÇÃO	unidade	1
21	Firewall – DATA CENTER TIPO I – AQUISIÇÃO	unidade	1
22	Firewall – DATA CENTER TIPO II - AQUISIÇÃO	unidade	1
23	Firewall – DATA CENTER TIPO III – AQUISIÇÃO	unidade	1
24	Gerência Centralizada e Relatoria – TIPO I – AQUISIÇÃO	unidade	4
25	Gerência Centralizada e Relatoria – TIPO II – AQUISIÇÃO	unidade	1

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

4.1. Especificação Detalhada:

4.1.1 É permitido a composição da solução ofertada entre diversos fabricantes, desde que não contemple solução de software livre;

4.1.2 Os firewalls ofertados devem ser tipo Next Generation Firewall (NGFW);

4.1.3 A comunicação entre os equipamentos de segurança e a solução de gerência deve ser através de meio criptografado;

4.1.4 Na data da proposta e durante a vigência do contrato, nenhum dos modelos ofertados poderão estar/serem listados no site do fabricante em listas de end-of-life, end-of-support e/ou end-of-sale;

4.1.5 O Throughput e as interfaces solicitados deverão ser comprovados através de datasheet público na internet. Caso haja divergência entre métricas do mesmo datasheet, será aceito o valor de maior capacidade.

4.1.6 **Item 01 -** Firewall – CENTRAL TIPO I

4.1.6.1 **Características Gerais**

4.1.6.1.1 Throughput de pelo menos 570 Mbps, com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação e prevenção de ameaças avançadas habilitados simultaneamente;

4.1.6.1.1.1 O Throughput é considerado como a quantidade de tráfego que um único equipamento consegue redirecionar. Não há soma entre o tráfego de entrada e de saída das interfaces;

4.1.6.1.2 Suportar pelo menos 3.100.000 (três milhões e cem mil) conexões ou sessões simultâneas;

4.1.6.1.3 Suportar pelo menos 45.000 (quarenta e cinco mil) novas conexões ou sessões por segundo;

4.1.6.1.4 Armazenamento interno em HDD ou SSD de pelo menos 240GB;

4.1.6.1.5 Possuir pelo menos 5 interfaces de rede 1G UTP;

4.1.6.1.6 Possuir 1 interface de rede dedicada ao gerenciamento;

4.1.6.1.7 Possuir 1 interface de rede dedicada para acesso via console;

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

4.1.6.1.8.1 Por funcionalidades de proteção de rede e próxima geração entende-se: reconhecimento e controle granular de aplicações, prevenção de ameaças, identificação de usuários, IPS e Firewall;

4.1.6.1.9 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;

4.1.6.1.10 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;

4.1.6.1.11 Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19", incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;

4.1.6.2 **Funcionalidades Genéricas de Firewall**

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

4.1.6.2.1.1 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;

4.1.6.2.1.2 Deve suportar os seguintes tipos de NAT:

4.1.6.2.1.3 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;

4.1.6.2.1.4 Enviar logs para sistemas de monitoração externos, simultaneamente;

4.1.6.2.1.5 Prover mecanismo de prevenção a ataques de falsificação de endereços (IP Spoofing) através da especificação da interface de rede pela qual uma comunicação deverá se originar;

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

4.1.6.2.1.7 Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);

4.1.6.2.1.8 Suportar OSPF graceful restart;

4.1.6.2.1.9 Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

4.1.6.3 **Funcionalidades de Filtro de Conteúdo Web**

4.1.6.3.1 Controle de políticas por aplicações, grupos de aplicações e categorias de aplicações;

4.1.6.3.2 Controle de políticas por usuários, grupos de usuários, IPs e redes;

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

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

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

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

4.1.6.3.5.2 Reconhecer pelo menos 2.900 (duas mil e novecentas) 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;

4.1.6.3.6 A checagem de assinaturas deve determinar se uma aplicação está utilizando a porta padrão ou não;

4.1.6.3.7 Para tráfego criptografado (SSL), deve de-criptografar pacotes a fim de possibilitar a leitura do payload para checagem de assinaturas de aplicações conhecidas;

4.1.6.3.8 Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo;

4.1.6.3.9 A decodificação de protocolo deve também identificar comportamentos específicos dentro da aplicação;

4.1.6.3.10 Atualizar a base de assinaturas de aplicações automaticamente;

4.1.6.3.11 Limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD;

4.1.6.3.12 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;

4.1.6.3.13 Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos ou análise heurística;

4.1.6.3.14 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 banco;

4.1.6.3.15 Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;

4.1.6.3.16 A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:

4.1.6.3.16.1 Permitir especificar política por tempo, com definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

4.1.6.3.16.2 Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes;

4.1.6.3.16.3 Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs atráves da integração com serviços de diretório, autenticação via Active Directory e base de dados local;

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

4.1.6.3.16.5 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;

4.1.6.3.16.6 Suportar base ou cache de URLs local no appliance, evitando atrasos de comunicação e validação das URLs;

4.1.6.3.16.7 Suportar a criação de categorias de URLs customizadas;

4.1.6.3.16.8 Suportar a exclusão de URLs do bloqueio, por categoria;

4.1.6.3.16.9 Permitir a customização de página de bloqueio;

4.1.6.3.17 Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, sem a necessidade de instalar nenhum cliente nos servidores Active Directory ou em outra máquina da rede;

4.1.6.3.18 Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via Radius ou syslog, para a identificação de endereços IP e usuários;

4.1.6.3.19 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);

4.1.6.4 **Funcionalidade de Prevenção de Ameaças**

4.1.6.4.1 Os dispositivos de proteção devem possuir módulo de IPS e suportar os módulos de: Antivírus e Anti-Malware integrados no próprio equipamento;

4.1.6.4.2 Deve incluir assinaturas de prevenção de intrusão (IPS) e suporte ao bloqueio de arquivos maliciosos (Antivírus e Anti-Malware);

4.1.6.4.3 Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Malware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;

4.1.6.4.4 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;

4.1.6.4.5 Deverá possuir os seguintes mecanismos de inspeção de IPS:

4.1.6.4.5.1 Análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;

4.1.6.4.6 Detectar e bloquear a origem de portscans;

4.1.6.4.7 Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações;

4.1.6.4.8 Possuir assinaturas para bloqueio de ataques de buffer overflow;
4.1.6.4.9 Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP;
4.1.6.4.10 Suportar bloqueio de arquivos por tipo;
4.1.6.4.11 Identificar e bloquear comunicação com botnets;
4.1.6.4.12 Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:
4.1.6.4.12.1 O nome da assinatura e do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo de proteção;
4.1.6.4.13 Deve suportar a captura de pacotes (PCAP), em assinatura de IPS e Anti-Malware;
4.1.6.4.14 Os eventos devem identificar o país de onde partiu a ameaça;
4.1.6.4.15 Suportar rastreamento de vírus em arquivos pdf;
4.1.6.4.16 Deve suportar a inspeção em arquivos comprimidos (zip, gzip,etc.);
4.1.6.4.17 Suportar a criação de políticas por Geo Localização, permitindo que o tráfego de determinado País/Países seja bloqueado;
4.1.6.4.18 Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
4.1.6.4.19 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;

4.1.6.5 **Prevenção de Ameaças Avançadas**
4.1.6.5.1 A solução deverá prover as funcionalidades de inspeção e prevenção de tráfego de entrada de malwares não conhecidos e do tipo APT, com filtro de ameaças avançadas e análise de execução em tempo real e inspeção com prevenção de tráfego de saída de callbacks (comunicação do malware com o servidor de comando e controle);
4.1.6.5.2 Implementar, identificar e bloquear malwares de dia zero em anexos de e-mail e URL's conhecidas;
4.1.6.5.3 A solução deve fornecer a capacidade de emular ataques em diferentes sistemas operacionais, dentre eles: Windows XP (32 bits), Windows 7 (32 e 64 bits), Windows 8, Windows 8.1 e Windows 10 (64 bits), assim como Office 2003, 2010 e 2013;
4.1.6.5.4 Implementar gerenciamento SNMP v2 e v3;
4.1.6.5.5 Implementar mecanismo de exceção, permitindo a criação de regras por VLAN, subrede e endereço IP;
4.1.6.5.6 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: cab, csv, doc, docx, docm, dot, dotm, dotx, exe, hwp, jar, pdf, pif, ppam, pps, ppsm, ppsx, potx, potm, ppt, pptm, pptx, rar, rtf, seven-z, sldm, sldx, swf, tar, tgz, xlam, xls, xlsx, xlt, xltx, xlsm, xltm, xll, xlsb, zip;
4.1.6.5.7 Prover informações para que a solução de relatórios possa apresentar via interface gráfica as seguintes informações:
4.1.6.5.7.1 Sumário executivo;
4.1.6.5.7.2 Relatório de máquinas infectadas;
4.1.6.5.7.3 Atividades do malware durante a execução de arquivo, nos ambientes controlados em todas as versões de sistemas operacionais requisitados neste projeto;
4.1.6.5.8 A solução deve permitir a criação de whitelists baseado no MD5 do arquivo;
4.1.6.5.9 Para melhor administração da solução, a solução deve possibilitar as seguintes visualizações a nível de monitoração:
4.1.6.5.9.1 Número de arquivos emulados;
4.1.6.5.10 A solução de possuir os indicadores abaixo referente ao último dia, última semana ou últimos 30 dias:
4.1.6.5.10.1 Arquivos scaneados;
4.1.6.5.10.2 Arquivos maliciosos;

4.1.6.6 **Controle de Qualidade de Serviço**

4.1.6.6.1 Suportar a criação de políticas de QoS por:
4.1.6.6.1.1 Endereço de origem, endereço de destino e por porta;
4.1.6.6.2 O QoS deve possibilitar a definição de classes por:
4.1.6.6.2.1 Banda garantida, banda máxima e fila de prioridade;
4.1.6.6.2.2 Disponibilizar estatísticas RealTime para classes de QoS;

4.1.6.7 **Funcionalidades de VPN**
4.1.6.7.1 Suportar VPN Site-to-Site e Client-To-Site;
4.1.6.7.2 Suportar IPSec VPN;
4.1.6.7.3 Suportar SSL VPN;
4.1.6.7.4 A VPN IPSEc deve suportar:
4.1.6.7.4.1 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;
4.1.6.7.5 **A VPN SSL deve suportar:**
4.1.6.7.5.1 Permitir que o usuário realize a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;
4.1.6.7.5.2 As funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;
4.1.6.7.5.3 Atribuição de endereço IP nos clientes remotos de VPN;
4.1.6.7.5.4 Atribuição de DNS nos clientes remotos de VPN;
4.1.6.7.5.5 Dever permitir criar políticas para tráfego dos clientes remotos conectados na VPN SSL;
4.1.6.7.5.6 Suportar autenticação via AD/LDAP, certificado digital e base de usuários local;
4.1.6.7.5.7 Suportar leitura e verificação de CRL (certificate revocation list);
4.1.6.7.5.8 O agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows XP, Vista, Windows 7, Windows 8 e MacOS X;

4.1.7 - **Item 02 -** Firewall – CENTRAL TIPO II

4.1.7.1 **Características Gerais**

4.1.7.1.1 Throughput de pelo menos 1 Gbps, com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação e prevenção de ameaças avançadas habilitados simultaneamente;
4.1.7.1.1.1 O Throughput é considerado como a quantidade de tráfego que um único equipamento consegue redirecionar. Não há soma entre o tráfego de entrada e de saída das interfaces;
4.1.7.1.2 Suportar pelo menos 3.100.000 (três milhões e cem mil) conexões ou sessões simultâneas;
4.1.7.1.3 Suportar pelo menos 120.000 (cento e vinte mil) novas conexões ou sessões por segundo;
4.1.7.1.4 Armazenamento interno em HDD ou SSD de pelo menos 240GB;
4.1.7.1.5 Possuir pelo menos 5 interfaces de rede 1G UTP;
4.1.7.1.6 Possuir 1 interface de rede dedicada ao gerenciamento;
4.1.7.1.7 Possuir 1 interface de rede dedicada para acesso via console;
4.1.7.1.8 Suportar até 20 (vinte) instâncias (contextos) virtuais de firewall;
4.1.7.1.9 A solução deve consistir de appliance de proteção de rede com funcionalidades de proteção de próxima geração;
4.1.7.1.9.1 Por funcionalidades de proteção de rede e próxima geração entende-se: reconhecimento e controle granular de aplicações, prevenção de ameaças, identificação de usuários, IPS e Firewall;
4.1.7.1.10 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;

4.1.7.1.11 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;

4.1.7.1.12 Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19", incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;

4.1.7.2 **Funcionalidades Genéricas de Firewall**

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

4.1.7.2.1.1 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;

4.1.7.2.1.2 **Deve suportar os seguintes tipos de NAT:**

4.1.7.2.1.3 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;

4.1.7.2.1.4 Enviar logs para sistemas de monitoração externos, simultaneamente;

4.1.7.2.1.5 Prover mecanismo de prevenção a ataques de falsificação de endereços (IP Spoofing) através da especificação da interface de rede pela qual uma comunicação deverá se originar;

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

4.1.7.2.1.7 Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);

4.1.7.2.1.8 Suportar OSPF graceful restart;

4.1.7.2.1.9 Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

4.1.7.3 **Funcionalidades de Filtro de Conteúdo Web**

4.1.7.3.1 Controle de políticas por aplicações, grupos de aplicações e categorias de aplicações;

4.1.7.3.2 Controle de políticas por usuários, grupos de usuários, IPs e redes;

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

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

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

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

4.1.7.3.5.2 Reconhecer pelo menos 2.900 (duas mil e novecentas) 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;

4.1.7.3.6 A checagem de assinaturas deve determinar se uma aplicação está utilizando a porta padrão ou não;

4.1.7.3.7 Para tráfego criptografado (SSL), deve de-criptografar pacotes a fim de possibilitar a leitura do payload para checagem de assinaturas de aplicações conhecidas;

4.1.7.3.8 Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo;

4.1.7.3.9 A decodificação de protocolo deve também identificar comportamentos específicos dentro da aplicação;

4.1.7.3.10 Atualizar a base de assinaturas de aplicações automaticamente;

4.1.7.3.11 Limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD;

4.1.7.3.12 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;

4.1.7.3.13 Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos ou análise heurística;

4.1.7.3.14 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 banco;

4.1.7.3.15 Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;

4.1.7.3.16 A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:

4.1.7.3.16.1 Permitir especificar política por tempo, com definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

4.1.7.3.16.2 Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes;

4.1.7.3.16.3 Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs atráves da integração com serviços de diretório, autenticação via Active Directory e base de dados local;

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

4.1.7.3.16.5 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;

4.1.7.3.16.6 Suportar base ou cache de URLs local no appliance, evitando atrasos de comunicação e validação das URLs;

4.1.7.3.16.7 Suportar a criação de categorias de URLs customizadas;

4.1.7.3.16.8 Suportar a exclusão de URLs do bloqueio, por categoria;

4.1.7.3.16.9 Permitir a customização de página de bloqueio;

4.1.7.3.17 Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, sem a necessidade de instalar nenhum cliente nos servidores Active Directory ou em outra máquina da rede;

4.1.7.3.18 Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via Radius ou syslog, para a identificação de endereços IP e usuários;

4.1.7.3.19 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);

4.1.7.4 **Funcionalidade de Prevenção de Ameaças**

4.1.7.4.1 Os dispositivos de proteção devem possuir módulo de IPS e suportar os módulos de: Antivírus e Anti-Malware integrados no próprio equipamento;

4.1.7.4.2 Deve incluir assinaturas de prevenção de intrusão (IPS) e suporte ao bloqueio de arquivos maliciosos (Antivírus e Anti-Malware);

4.1.7.4.3 Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Malware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;

4.1.7.4.4 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;

4.1.7.4.5 Deverá possuir os seguintes mecanismos de inspeção de IPS:

4.1.7.4.5.1 Análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;

4.1.7.4.6 Detectar e bloquear a origem de portscans;

4.1.7.4.7 Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações;

4.1.7.4.8 Possuir assinaturas para bloqueio de ataques de buffer overflow;
4.1.7.4.9 Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP;
4.1.7.4.10 Suportar bloqueio de arquivos por tipo;
4.1.7.4.11 Identificar e bloquear comunicação com botnets;
4.1.7.4.12 Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:
4.1.7.4.12.1 O nome da assinatura e do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo de proteção;
4.1.7.4.13 Deve suportar a captura de pacotes (PCAP), em assinatura de IPS e Anti-Malware;
4.1.7.4.14 Os eventos devem identificar o país de onde partiu a ameaça;
4.1.7.4.15 Suportar rastreamento de vírus em arquivos pdf;
4.1.7.4.16 Deve suportar a inspeção em arquivos comprimidos (zip, gzip,etc.);
4.1.7.4.17 Suportar a criação de políticas por Geo Localização, permitindo que o tráfego de determinado País/Países seja bloqueado;
4.1.7.4.18 Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
4.1.7.4.19 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;

4.1.7.5 **Prevenção de Ameaças Avançadas**
4.1.7.5.1 A solução deverá prover as funcionalidades de inspeção e prevenção de tráfego de entrada de malwares não conhecidos e do tipo APT, com filtro de ameaças avançadas e análise de execução em tempo real e inspeção com prevenção de tráfego de saída de callbacks (comunicação do malware com o servidor de comando e controle);
4.1.7.5.2 Implementar, identificar e bloquear malwares de dia zero em anexos de e-mail e URL's conhecidas;
4.1.7.5.3 A solução deve fornecer a capacidade de emular ataques em diferentes sistemas operacionais, dentre eles: Windows XP (32 bits), Windows 7 (32 e 64 bits), Windows 8, Windows 8.1 e Windows 10 (64 bits), assim como Office 2003, 2010 e 2013;
4.1.7.5.4 Implementar gerenciamento SNMP v2 e v3;
4.1.7.5.5 Implementar mecanismo de exceção, permitindo a criação de regras por VLAN, subrede e endereço IP;
4.1.7.5.6 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: cab, csv, doc, docx, docm, dot, dotm, dotx, exe, hwp, jar, pdf, pif, ppam, pps, ppsm, ppsx, potx, potm, ppt, pptm, pptx, rar, rtf, seven-z, sldm, sldx, swf, tar, tgz, xlam, xls, xlsx, xlt, xltx, xlsm, xltm, xll, xlsb, zip;
4.1.7.5.7 Prover informações para que a solução de relatórios possa apresentar via interface gráfica as seguintes informações:
4.1.7.5.7.1 Sumário executivo;
4.1.7.5.7.2 Relatório de máquinas infectadas;
4.1.7.5.7.3 Atividades do malware durante a execução de arquivo, nos ambientes controlados em todas as versões de sistemas operacionais requisitados neste projeto;
4.1.7.5.8 A solução deve permitir a criação de whitelists baseado no MD5 do arquivo;
4.1.7.5.9 Para melhor administração da solução, a solução deve possibilitar as seguintes visualizações a nível de monitoração:
4.1.7.5.9.1 Número de arquivos emulados;
4.1.7.5.10 A solução de possuir os indicadores abaixo referente ao último dia, última semana ou últimos 30 dias:
4.1.7.5.10.1 Arquivos scaneados;
4.1.7.5.10.2 Arquivos maliciosos;

4.1.7.6 **Controle de Qualidade de Serviço**

4.1.7.6.1 Suportar a criação de políticas de QoS por:
4.1.7.6.1.1 Endereço de origem, endereço de destino e por porta;
4.1.7.6.2 O QoS deve possibilitar a definição de classes por:
4.1.7.6.2.1 Banda garantida, banda máxima e fila de prioridade;
4.1.7.6.2.2 Disponibilizar estatísticas RealTime para classes de QoS;

4.1.7.7 **Funcionalidades de VPN**
4.1.7.7.1 Suportar VPN Site-to-Site e Client-To-Site;
4.1.7.7.2 Suportar IPSec VPN;
4.1.7.7.3 Suportar SSL VPN;
4.1.7.7.4 **A VPN IPSEc deve suportar:**
4.1.7.7.4.1 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;
4.1.7.7.5 **A VPN SSL deve suportar:**
4.1.7.7.5.1 Permitir que o usuário realize a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;
4.1.7.7.5.2 A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;
4.1.7.7.5.3 Atribuição de endereço IP nos clientes remotos de VPN;
4.1.7.7.5.4 Atribuição de DNS nos clientes remotos de VPN;
4.1.7.7.5.5 Dever permitir criar políticas para tráfego dos clientes remotos conectados na VPN SSL;
4.1.7.7.5.6 Suportar autenticação via AD/LDAP, certificado digital e base de usuários local;
4.1.7.7.5.7 Suportar leitura e verificação de CRL (certificate revocation list);
4.1.7.7.5.8 O agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows XP, Vista, Windows 7, Windows 8 e MacOS X;

4.1.8 - **Item 03 -** Firewall – CENTRAL TIPO III

4.1.8.1 **Características Gerais**
4.1.8.1.1 Throughput de pelo menos 2.7 Gbps, com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação e prevenção de ameaças avançadas habilitados simultaneamente;
4.1.8.1.1.1 O Throughput é considerado como a quantidade de tráfego que um único equipamento consegue redirecionar. Não há soma entre o tráfego de entrada e de saída das interfaces;
4.1.8.1.2 Suportar pelo menos 3.100.000 (três milhões e cem mil) conexões ou sessões simultâneas;
4.1.8.1.3 Suportar pelo menos 180.000 (cento e oitenta mil) novas conexões ou sessões por segundo;
4.1.8.1.4 Armazenamento interno em HDD ou SSD de pelo menos 240GB;
4.1.8.1.5 Possuir pelo menos 8 interfaces de rede 1G UTP;
4.1.8.1.6 Possuir 1 interface de rede dedicada ao sincronismo;
4.1.8.1.7 Possuir 1 interface de rede dedicada ao gerenciamento;
4.1.8.1.8 Possuir 1 interface de rede dedicada para acesso via console;
4.1.8.1.9 Suportar até 20 (vinte) instâncias (contextos) virtuais de firewall;
4.1.8.1.10 A solução deve consistir de appliance de proteção de rede com funcionalidades de proteção de próxima geração;
4.1.8.1.10.1 Por funcionalidades de proteção de rede e próxima geração entende-se: reconhecimento e controle granular de aplicações, prevenção de ameaças, identificação de usuários, IPS e Firewall;
4.1.8.1.11 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;

4.1.8.1.12 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;

4.1.8.1.13 Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19", incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;

4.1.8.2 **Funcionalidades Genéricas de Firewall**

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

4.1.8.2.1.1 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;

4.1.8.2.1.2 **Deve suportar os seguintes tipos de NAT:**

4.1.8.2.1.3 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;

4.1.8.2.1.4 Enviar logs para sistemas de monitoração externos, simultaneamente;

4.1.8.2.1.5 Prover mecanismo de prevenção a ataques de falsificação de endereços (IP Spoofing) através da especificação da interface de rede pela qual uma comunicação deverá se originar;

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

4.1.8.2.1.7 Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);

4.1.8.2.1.8 Suportar OSPF graceful restart;

4.1.8.2.1.9 Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

4.1.8.3 **Funcionalidades de Filtro de Conteúdo Web**

4.1.8.3.1 Controle de políticas por aplicações, grupos de aplicações e categorias de aplicações;

4.1.8.3.2 Controle de políticas por usuários, grupos de usuários, IPs e redes;

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

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

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

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

4.1.8.3.5.2 Reconhecer pelo menos 2.900 (duas mil e novecentas) 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;

4.1.8.3.6 A checagem de assinaturas deve determinar se uma aplicação está utilizando a porta padrão ou não;

4.1.8.3.7 Para tráfego criptografado (SSL), deve de-criptografar pacotes a fim de possibilitar a leitura do payload para checagem de assinaturas de aplicações conhecidas;

4.1.8.3.8 Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo;

4.1.8.3.9 A decodificação de protocolo deve também identificar comportamentos específicos dentro da aplicação;

4.1.8.3.10 Atualizar a base de assinaturas de aplicações automaticamente;

4.1.8.3.11 Limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD;

4.1.8.3.12 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;

4.1.8.3.13 Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos ou análise heurística;

4.1.8.3.14 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 banco;

4.1.8.3.15 Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;

4.1.8.3.16 **A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:**

4.1.8.3.16.1 Permitir especificar política por tempo, com definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

4.1.8.3.16.2 Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes;

4.1.8.3.16.3 Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs atráves da integração com serviços de diretório, autenticação via Active Directory e base de dados local;

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

4.1.8.3.16.5 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;

4.1.8.3.16.6 Suportar base ou cache de URLs local no appliance, evitando atrasos de comunicação e validação das URLs;

4.1.8.3.16.7 Suportar a criação de categorias de URLs customizadas;

4.1.8.3.16.8 Suportar a exclusão de URLs do bloqueio, por categoria;

4.1.8.3.16.9 Permitir a customização de página de bloqueio;

4.1.8.3.17 Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, sem a necessidade de instalar nenhum cliente nos servidores Active Directory ou em outra máquina da rede;

4.1.8.3.18 Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via Radius ou syslog, para a identificação de endereços IP e usuários;

4.1.8.3.19 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);

4.1.8.4 **Funcionalidade de Prevenção de Ameaças**

4.1.8.4.1 Os dispositivos de proteção devem possuir módulo de IPS e suportar os módulos de: Antivírus e Anti-Malware integrados no próprio equipamento;

4.1.8.4.2 Deve incluir assinaturas de prevenção de intrusão (IPS) e suporte ao bloqueio de arquivos maliciosos (Antivírus e Anti-Malware);

4.1.8.4.3 Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Malware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;

4.1.8.4.4 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;

4.1.8.4.5 Deverá possuir os seguintes mecanismos de inspeção de IPS:

4.1.8.4.5.1 Análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;

4.1.8.4.6 Detectar e bloquear a origem de portscans;

4.1.8.4.7 Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações;
4.1.8.4.8 Possuir assinaturas para bloqueio de ataques de buffer overflow;
4.1.8.4.9 Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP;
4.1.8.4.10 Suportar bloqueio de arquivos por tipo;
4.1.8.4.11 Identificar e bloquear comunicação com botnets;
4.1.8.4.12 Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:
4.1.8.4.12.1 O nome da assinatura e do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo de proteção;
4.1.8.4.13 Deve suportar a captura de pacotes (PCAP), em assinatura de IPS e Anti-Malware;
4.1.8.4.14 Os eventos devem identificar o país de onde partiu a ameaça;
4.1.8.4.15 Suportar rastreamento de vírus em arquivos pdf;
4.1.8.4.16 Deve suportar a inspeção em arquivos comprimidos (zip, gzip,etc.);
4.1.8.4.17 Suportar a criação de políticas por Geo Localização, permitindo que o tráfego de determinado País/Países seja bloqueado;
4.1.8.4.18 Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
4.1.8.4.19 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;

4.1.8.5 **Prevenção de Ameaças Avançadas**
4.1.8.5.1 A solução deverá prover as funcionalidades de inspeção e prevenção de tráfego de entrada de malwares não conhecidos e do tipo APT, com filtro de ameaças avançadas e análise de execução em tempo real e inspeção com prevenção de tráfego de saída de callbacks (comunicação do malware com o servidor de comando e controle);
4.1.8.5.2 Implementar, identificar e bloquear malwares de dia zero em anexos de e-mail e URL's conhecidas;
4.1.8.5.3 A solução deve fornecer a capacidade de emular ataques em diferentes sistemas operacionais, dentre eles: Windows XP (32 bits), Windows 7 (32 e 64 bits), Windows 8, Windows 8.1 e Windows 10 (64 bits), assim como Office 2003, 2010 e 2013;
4.1.8.5.4 Implementar gerenciamento SNMP v2 e v3;
4.1.8.5.5 Implementar mecanismo de exceção, permitindo a criação de regras por VLAN, subrede e endereço IP;
4.1.8.5.6 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: cab, csv, doc, docx, docm, dot, dotm, dotx, exe, hwp, jar, pdf, pif, ppam, pps, ppsm, ppsx, potx, potm, ppt, pptm, pptx, rar, rtf, seven-z, sldm, sldx, swf, tar, tgz, xlam, xls, xlsx, xlt, xltx, xlsm, xltm, xll, xlsb, zip;
4.1.8.5.7 **Prover informações para que a solução de relatórios possa apresentar via interface gráfica as seguintes informações:**
4.1.8.5.7.1 Sumário executivo;
4.1.8.5.7.2 Relatório de máquinas infectadas;
4.1.8.5.7.3 Atividades do malware durante a execução de arquivo, nos ambientes controlados em todas as versões de sistemas operacionais requisitados neste projeto;
4.1.8.5.8 A solução deve permitir a criação de whitelists baseado no MD5 do arquivo;
4.1.8.5.9 Para melhor administração da solução, a solução deve possibilitar as seguintes visualizações a nível de monitoração:
4.1.8.5.9.1 Número de arquivos emulados;
4.1.8.5.10 A solução de possuir os indicadores abaixo referente ao último dia, última semana ou últimos 30 dias:
4.1.8.5.10.1 Arquivos scaneados;
4.1.8.5.10.2 Arquivos maliciosos;

4.1.8.6 **Controle de Qualidade de Serviço**

4.1.8.6.1 Suportar a criação de políticas de QoS por:

4.1.8.6.1.1 Endereço de origem, endereço de destino e por porta;

4.1.8.6.2 O QoS deve possibilitar a definição de classes por:

4.1.8.6.2.1 Banda garantida, banda máxima e fila de prioridade;

4.1.8.6.2.2 Disponibilizar estatísticas RealTime para classes de QoS;

4.1.8.7 **Funcionalidades de VPN**

4.1.8.7.1 Suportar VPN Site-to-Site e Client-To-Site;

4.1.8.7.2 Suportar IPSec VPN;

4.1.8.7.3 Suportar SSL VPN;

4.1.8.7.4 A VPN IPSEc deve suportar:

4.1.8.7.4.1 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;

4.1.8.7.5 **A VPN SSL deve suportar:**

4.1.8.7.5.1 Permitir que o usuário realize a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;

4.1.8.7.5.2 As funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;

4.1.8.7.5.3 Atribuição de endereço IP nos clientes remotos de VPN;

4.1.8.7.5.4 Atribuição de DNS nos clientes remotos de VPN;

4.1.8.7.5.5 Dever permitir criar políticas para tráfego dos clientes remotos conectados na VPN SSL;

4.1.8.7.5.6 Suportar autenticação via AD/LDAP, certificado digital e base de usuários local;

4.1.8.7.5.7 Suportar leitura e verificação de CRL (certificate revocation list);

4.1.8.7.5.8 O agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows XP, Vista, Windows 7, Windows 8 e MacOS X;

4.1.9 - **Item 04 -** Firewall – CENTRAL TIPO IV

4.1.9.1 **Características Gerais**

4.1.9.1.1 Throughput de pelo menos 6 Gbps, com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação e prevenção de ameaças avançadas habilitados simultaneamente;

4.1.9.1.1.1 O Throughput é considerado como a quantidade de tráfego que um único equipamento consegue redirecionar. Não há soma entre o tráfego de entrada e de saída das interfaces;

4.1.9.1.2 Suportar pelo menos 3.100.000 (três milhões e cem mil) conexões ou sessões simultâneas;

4.1.9.1.3 Suportar pelo menos 205.000 (duzentas e cinco mil) novas conexões ou sessões por segundo;

4.1.9.1.4 Armazenamento interno em HDD ou SSD de pelo menos 480 GB;

4.1.9.1.5 Possuir pelo menos 8 interfaces de rede 1G UTP;

4.1.9.1.6 Deve suportar expansão para portas 10G SFP+;

4.1.9.1.7 Deve suportar expansão para portas 40G QSFP+;

4.1.9.1.8 Possuir 1 interface de rede dedicada ao sincronismo;

4.1.9.1.9 Possuir 1 interface de rede dedicada ao gerenciamento;

4.1.9.1.10 Possuir 1 interface de rede dedicada para acesso via console;

4.1.9.1.11 Suportar até 20 (vinte) instâncias (contextos) virtuais de firewall;

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

4.1.9.1.12.1 Por funcionalidades de proteção de rede e próxima geração entende-se: reconhecimento e controle granular de aplicações, prevenção de ameaças, identificação de usuários, IPS e Firewall;

4.1.9.1.13 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;

4.1.9.1.14 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;

4.1.9.1.15 Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19", incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;

4.1.9.2 **Funcionalidades Genéricas de Firewall**

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

4.1.9.2.1.1 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;

4.1.9.2.1.2 Deve suportar os seguintes tipos de NAT:

4.1.9.2.1.3 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;

4.1.9.2.1.4 Enviar logs para sistemas de monitoração externos, simultaneamente;

4.1.9.2.1.5 Prover mecanismo de prevenção a ataques de falsificação de endereços (IP Spoofing) através da especificação da interface de rede pela qual uma comunicação deverá se originar;

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

4.1.9.2.1.7 Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);

4.1.9.2.1.8 Suportar OSPF graceful restart;

4.1.9.2.1.9 Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

4.1.9.3 **Funcionalidades de Filtro de Conteúdo Web**

4.1.9.3.1 Controle de políticas por aplicações, grupos de aplicações e categorias de aplicações;

4.1.9.3.2 Controle de políticas por usuários, grupos de usuários, IPs e redes;

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

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

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

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

4.1.9.3.5.2 Reconhecer pelo menos 2.900 (duas mil e novecentas) 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;

4.1.9.3.6 A checagem de assinaturas deve determinar se uma aplicação está utilizando a porta padrão ou não;

4.1.9.3.7 Para tráfego criptografado (SSL), deve de-criptografar pacotes a fim de possibilitar a leitura do payload para checagem de assinaturas de aplicações conhecidas;

4.1.9.3.8 Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo;

4.1.9.3.9 A decodificação de protocolo deve também identificar comportamentos específicos dentro da aplicação;

4.1.9.3.10 Atualizar a base de assinaturas de aplicações automaticamente;

4.1.9.3.11 Limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD;

4.1.9.3.12 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;

4.1.9.3.13 Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos ou análise heurística;

4.1.9.3.14 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 banco;

4.1.9.3.15 Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;

4.1.9.3.16 A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:

4.1.9.3.16.1 Permitir especificar política por tempo, com definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

4.1.9.3.16.2 Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes;

4.1.9.3.16.3 Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs atráves da integração com serviços de diretório, autenticação via Active Directory e base de dados local;

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

4.1.9.3.16.5 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;

4.1.9.3.16.6 Suportar base ou cache de URLs local no appliance, evitando atrasos de comunicação e validação das URLs;

4.1.9.3.16.7 Suportar a criação de categorias de URLs customizadas;

4.1.9.3.16.8 Suportar a exclusão de URLs do bloqueio, por categoria;

4.1.9.3.16.9 Permitir a customização de página de bloqueio;

4.1.9.3.17 Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, sem a necessidade de instalar nenhum cliente nos servidores Active Directory ou em outra máquina da rede;

4.1.9.3.18 Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via Radius ou syslog, para a identificação de endereços IP e usuários;

4.1.9.3.19 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);

4.1.9.4 **Funcionalidade de Prevenção de Ameaças**

4.1.9.4.1 Os dispositivos de proteção devem possuir módulo de IPS e suportar os módulos de: Antivírus e Anti-Malware integrados no próprio equipamento;

4.1.9.4.2 Deve incluir assinaturas de prevenção de intrusão (IPS) e suporte ao bloqueio de arquivos maliciosos (Antivírus e Anti-Malware);

4.1.9.4.3 Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Malware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;

4.1.9.4.4 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;

4.1.9.4.5 Deverá possuir os seguintes mecanismos de inspeção de IPS:

4.1.9.4.5.1 Análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;

4.1.9.4.6 Detectar e bloquear a origem de portscans;

4.1.9.4.7 Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações;
4.1.9.4.8 Possuir assinaturas para bloqueio de ataques de buffer overflow;
4.1.9.4.9 Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP;
4.1.9.4.10 Suportar bloqueio de arquivos por tipo;
4.1.9.4.11 Identificar e bloquear comunicação com botnets;
4.1.9.4.12 Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:
4.1.9.4.12.1 O nome da assinatura e do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo de proteção;
4.1.9.4.13 Deve suportar a captura de pacotes (PCAP), em assinatura de IPS e Anti-Malware;
4.1.9.4.14 Os eventos devem identificar o país de onde partiu a ameaça;
4.1.9.4.15 Suportar rastreamento de vírus em arquivos pdf;
4.1.9.4.16 Deve suportar a inspeção em arquivos comprimidos (zip, gzip,etc.);
4.1.9.4.17 Suportar a criação de políticas por Geo Localização, permitindo que o tráfego de determinado País/Países seja bloqueado;
4.1.9.4.18 Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
4.1.9.4.19 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;

4.1.9.5 **Prevenção de Ameaças Avançadas**
4.1.9.5.1 A solução deverá prover as funcionalidades de inspeção e prevenção de tráfego de entrada de malwares não conhecidos e do tipo APT, com filtro de ameaças avançadas e análise de execução em tempo real e inspeção com prevenção de tráfego de saída de callbacks (comunicação do malware com o servidor de comando e controle);
4.1.9.5.2 Implementar, identificar e bloquear malwares de dia zero em anexos de e-mail e URL's conhecidas;
4.1.9.5.3 A solução deve fornecer a capacidade de emular ataques em diferentes sistemas operacionais, dentre eles: Windows XP (32 bits), Windows 7 (32 e 64 bits), Windows 8, Windows 8.1 e Windows 10 (64 bits), assim como Office 2003, 2010 e 2013;
4.1.9.5.4 Implementar gerenciamento SNMP v2 e v3;
4.1.9.5.5 Implementar mecanismo de exceção, permitindo a criação de regras por VLAN, subrede e endereço IP;
4.1.9.5.6 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: cab, csv, doc, docx, docm, dot, dotm, dotx, exe, hwp, jar, pdf, pif, ppam, pps, ppsm, ppsx, potx, potm, ppt, pptm, pptx, rar, rtf, seven-z, sldm, sldx, swf, tar, tgz, xlam, xls, xlsx, xlt, xltx, xlsm, xltm, xll, xlsb, zip;
4.1.9.5.7 **Prover informações para que a solução de relatórios possa apresentar via interface gráfica as seguintes informações:**
4.1.9.5.7.1 Sumário executivo;
4.1.9.5.7.2 Relatório de máquinas infectadas;
4.1.9.5.7.3 Atividades do malware durante a execução de arquivo, nos ambientes controlados em todas as versões de sistemas operacionais requisitados neste projeto;
4.1.9.5.8 A solução deve permitir a criação de whitelists baseado no MD5 do arquivo;
4.1.9.5.9 Para melhor administração da solução, a solução deve possibilitar as seguintes visualizações a nível de monitoração:
4.1.9.5.9.1 Número de arquivos emulados;
4.1.9.5.10 A solução de possuir os indicadores abaixo referente ao último dia, última semana ou últimos 30 dias:
4.1.9.5.10.1 Arquivos scaneados;
4.1.9.5.10.2 Arquivos maliciosos;

4.1.9.6 **Controle de Qualidade de Serviço**

4.1.9.6.1 Suportar a criação de políticas de QoS por:

4.1.9.6.1.1 Endereço de origem, endereço de destino e por porta;

4.1.9.6.2 O QoS deve possibilitar a definição de classes por:

4.1.9.6.2.1 Banda garantida, banda máxima e fila de prioridade;

4.1.9.6.2.2 Disponibilizar estatísticas RealTime para classes de QoS;

4.1.9.7 **Funcionalidades de VPN**

4.1.9.7.1 Suportar VPN Site-to-Site e Client-To-Site;

4.1.9.7.2 Suportar IPSec VPN;

4.1.9.7.3 Suportar SSL VPN;

4.1.9.7.4 **A VPN IPSEc deve suportar:**

4.1.9.7.4.1 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;

4.1.9.7.5 A VPN SSL deve suportar:

4.1.9.7.5.1 Permitir que o usuário realize a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;

4.1.9.7.5.2 A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;

4.1.9.7.5.3 Atribuição de endereço IP nos clientes remotos de VPN;

4.1.9.7.5.4 Atribuição de DNS nos clientes remotos de VPN;

4.1.9.7.5.5 Dever permitir criar políticas para tráfego dos clientes remotos conectados na VPN SSL;

4.1.9.7.5.6 Suportar autenticação via AD/LDAP, certificado digital e base de usuários local;

4.1.9.7.5.7 Suportar leitura e verificação de CRL (certificate revocation list);

4.1.9.7.5.8 O agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows XP, Vista, Windows 7, Windows 8 e MacOS X;

4.1.10 - **Item 05 -** Firewall – DATA CENTER TIPO I

4.1.10.1 **Características Gerais**

4.1.10.1.1 Throughput de pelo menos 8.8 Gbps, com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação e prevenção de ameaças avançadas habilitados simultaneamente;

4.1.10.1.1.1 O Throughput é considerado como a quantidade de tráfego que um único equipamento consegue redirecionar. Não há soma entre o tráfego de entrada e de saída das interfaces;

4.1.10.1.2 Suportar pelo menos 8.000.000 (oito milhões) de conexões ou sessões simultâneas;

4.1.10.1.3 Suportar pelo menos 295.000 (duzentas e noventa e cinco mil) novas conexões ou sessões por segundo;

4.1.10.1.4 Armazenamento interno em HDD ou SSD de pelo menos 480 GB;

4.1.10.1.5 Possuir pelo menos 8 interfaces de rede 1G UTP;

4.1.10.1.6 Deve suportar expansão para portas 10G SFP+;

4.1.10.1.7 Deve suportar expansão para portas 40G QSFP+;

4.1.10.1.8 Possuir 1 interface de rede dedicada ao sincronismo;

4.1.10.1.9 Possuir 1 interface de rede dedicada ao gerenciamento;

4.1.10.1.10 Possuir 1 interface de rede dedicada para acesso via console;

4.1.10.1.11 Suportar até 30 (trinta) instâncias (contextos) virtuais de firewall;

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

4.1.10.1.12.1 Por funcionalidades de proteção de rede e próxima geração entende-se: reconhecimento e controle granular de aplicações, prevenção de ameaças, identificação de usuários, IPS e Firewall;

4.1.10.1.13 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;

4.1.10.1.14 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;

4.1.10.1.15 Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19", incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;

4.1.10.2 **Funcionalidades Genéricas de Firewall**

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

4.1.10.2.1.1 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;

4.1.10.2.1.2 **Deve suportar os seguintes tipos de NAT:**

4.1.10.2.1.3 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;

4.1.10.2.1.4 Enviar logs para sistemas de monitoração externos, simultaneamente;

4.1.10.2.1.5 Prover mecanismo de prevenção a ataques de falsificação de endereços (IP Spoofing) através da especificação da interface de rede pela qual uma comunicação deverá se originar;

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

4.1.10.2.1.7 Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);

4.1.10.2.1.8 Suportar OSPF graceful restart;

4.1.10.2.1.9 Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

4.1.10.3 **Funcionalidades de Filtro de Conteúdo Web**

4.1.10.3.1 Controle de políticas por aplicações, grupos de aplicações e categorias de aplicações;

4.1.10.3.2 Controle de políticas por usuários, grupos de usuários, IPs e redes;

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

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

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

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

4.1.10.3.5.2 Reconhecer pelo menos 2.900 (duas mil e novecentas) 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;

4.1.10.3.6 A checagem de assinaturas deve determinar se uma aplicação está utilizando a porta padrão ou não;

4.1.10.3.7 Para tráfego criptografado (SSL), deve de-criptografar pacotes a fim de possibilitar a leitura do payload para checagem de assinaturas de aplicações conhecidas;

4.1.10.3.8 Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo;

4.1.10.3.9 A decodificação de protocolo deve também identificar comportamentos específicos dentro da aplicação;

4.1.10.3.10 Atualizar a base de assinaturas de aplicações automaticamente;

4.1.10.3.11 Limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD;

4.1.10.3.12 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;

4.1.10.3.13 Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos ou análise heurística;

4.1.10.3.14 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 banco;

4.1.10.3.15 Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;

4.1.10.3.16 A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:

4.1.10.3.16.1 Permitir especificar política por tempo, com definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

4.1.10.3.16.2 Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes;

4.1.10.3.16.3 Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs atráves da integração com serviços de diretório, autenticação via Active Directory e base de dados local;

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

4.1.10.3.16.5 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;

4.1.10.3.16.6 Suportar base ou cache de URLs local no appliance, evitando atrasos de comunicação e validação das URLs;

4.1.10.3.16.7 Suportar a criação de categorias de URLs customizadas;

4.1.10.3.16.8 Suportar a exclusão de URLs do bloqueio, por categoria;

4.1.10.3.16.9 Permitir a customização de página de bloqueio;

4.1.10.3.17 Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, sem a necessidade de instalar nenhum cliente nos servidores Active Directory ou em outra máquina da rede;

4.1.10.3.18 Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via Radius ou syslog, para a identificação de endereços IP e usuários;

4.1.10.3.19 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);

4.1.10.4 **Funcionalidade de Prevenção de Ameaças**

4.1.10.4.1 Os dispositivos de proteção devem possuir módulo de IPS e suportar os módulos de: Antivírus e Anti-Malware integrados no próprio equipamento;

4.1.10.4.2 Deve incluir assinaturas de prevenção de intrusão (IPS) e suporte ao bloqueio de arquivos maliciosos (Antivírus e Anti-Malware);

4.1.10.4.3 Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Malware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;

4.1.10.4.4 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;

4.1.10.4.5 Deverá possuir os seguintes mecanismos de inspeção de IPS:

4.1.10.4.5.1 Análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;

4.1.10.4.6 Detectar e bloquear a origem de portscans;

4.1.10.4.7 Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações;
4.1.10.4.8 Possuir assinaturas para bloqueio de ataques de buffer overflow;
4.1.10.4.9 Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP;
4.1.10.4.10 Suportar bloqueio de arquivos por tipo;
4.1.10.4.11 Identificar e bloquear comunicação com botnets;
4.1.10.4.12 Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:
4.1.10.4.12.1 O nome da assinatura e do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo de proteção;
4.1.10.4.13 Deve suportar a captura de pacotes (PCAP), em assinatura de IPS e Anti-Malware;
4.1.10.4.14 Os eventos devem identificar o país de onde partiu a ameaça;
4.1.10.4.15 Suportar rastreamento de vírus em arquivos pdf;
4.1.10.4.16 Deve suportar a inspeção em arquivos comprimidos (zip, gzip,etc.);
4.1.10.4.17 Suportar a criação de políticas por Geo Localização, permitindo que o tráfego de determinado País/Países seja bloqueado;
4.1.10.4.18 Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
4.1.10.4.19 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;

4.1.10.5 **Prevenção de Ameaças Avançadas**
4.1.10.5.1 A solução deverá prover as funcionalidades de inspeção e prevenção de tráfego de entrada de malwares não conhecidos e do tipo APT, com filtro de ameaças avançadas e análise de execução em tempo real e inspeção com prevenção de tráfego de saída de callbacks (comunicação do malware com o servidor de comando e controle);
4.1.10.5.2 Implementar, identificar e bloquear malwares de dia zero em anexos de e-mail e URL's conhecidas;
4.1.10.5.3 A solução deve fornecer a capacidade de emular ataques em diferentes sistemas operacionais, dentre eles: Windows XP (32 bits), Windows 7 (32 e 64 bits), Windows 8, Windows 8.1 e Windows 10 (64 bits), assim como Office 2003, 2010 e 2013;
4.1.10.5.4 Implementar gerenciamento SNMP v2 e v3;
4.1.10.5.5 Implementar mecanismo de exceção, permitindo a criação de regras por VLAN, subrede e endereço IP;
4.1.10.5.6 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: cab, csv, doc, docx, docm, dot, dotm, dotx, exe, hwp, jar, pdf, pif, ppam, pps, ppsm, ppsx, potx, potm, ppt, pptm, pptx, rar, rtf, seven-z, sldm, sldx, swf, tar, tgz, xlam, xls, xlsx, xlt, xltx, xlsm, xltm, xll, xlsb, zip;
4.1.10.5.7 Prover informações para que a solução de relatórios possa apresentar via interface gráfica as seguintes informações:
4.1.10.5.7.1 Sumário executivo;
4.1.10.5.7.2 Relatório de máquinas infectadas;
4.1.10.5.7.3 Atividades do malware durante a execução de arquivo, nos ambientes controlados em todas as versões de sistemas operacionais requisitados neste projeto;
4.1.10.5.8 A solução deve permitir a criação de whitelists baseado no MD5 do arquivo;
4.1.10.5.9 Para melhor administração da solução, a solução deve possibilitar as seguintes visualizações a nível de monitoração:
4.1.10.5.9.1 Número de arquivos emulados;
4.1.10.5.10 A solução de possuir os indicadores abaixo referente ao último dia, última semana ou últimos 30 dias:
4.1.10.5.10.1 Arquivos scaneados;
4.1.10.5.10.2 Arquivos maliciosos;

4.1.10.6 **Controle de Qualidade de Serviço**

4.1.10.6.1 Suportar a criação de políticas de QoS por:

4.1.10.6.1.1 Endereço de origem, endereço de destino e por porta;

4.1.10.6.2 O QoS deve possibilitar a definição de classes por:

4.1.10.6.2.1 Banda garantida, banda máxima e fila de prioridade;

4.1.10.6.2.2 Disponibilizar estatísticas RealTime para classes de QoS;

4.1.10.7 **Funcionalidades de VPN**

4.1.10.7.1 Suportar VPN Site-to-Site e Client-To-Site;

4.1.10.7.2 Suportar IPSec VPN;

4.1.10.7.3 Suportar SSL VPN;

4.1.10.7.4 **A VPN IPSEc deve suportar:**

4.1.10.7.4.1 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;

4.1.10.7.5 **A VPN SSL deve suportar:**

4.1.10.7.5.1 Permitir que o usuário realize a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;

4.1.10.7.5.2 A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;

4.1.10.7.5.3 Atribuição de endereço IP nos clientes remotos de VPN;

4.1.10.7.5.4 Atribuição de DNS nos clientes remotos de VPN;

4.1.10.7.5.5 Dever permitir criar políticas para tráfego dos clientes remotos conectados na VPN SSL;

4.1.10.7.5.6 Suportar autenticação via AD/LDAP, certificado digital e base de usuários local;

4.1.10.7.5.7 Suportar leitura e verificação de CRL (certificate revocation list);

4.1.10.7.5.8 O agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows XP, Vista, Windows 7, Windows 8 e MacOS X;

4.1.11 - **Item 06 -** Firewall – DATA CENTER TIPO II

4.1.11.1 **Características Gerais**

4.1.11.1.1 Throughput de pelo menos 11 Gbps, com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação e prevenção de ameaças avançadas habilitados simultaneamente;

4.1.11.1.1.1 O Throughput é considerado como a quantidade de tráfego que um único equipamento consegue redirecionar. Não há soma entre o tráfego de entrada e de saída das interfaces;

4.1.11.1.2 Suportar pelo menos 7.900.000 (sete milhões e novecentas mil) conexões ou sessões simultâneas;

4.1.11.1.3 Suportar pelo menos 370.000 (trezentos e setenta mil) novas conexões ou sessões por segundo;

4.1.11.1.4 Armazenamento interno em HDD ou SSD de pelo menos 480 GB;

4.1.11.1.5 Possuir pelo menos 8 interfaces de rede 1G UTP;

4.1.11.1.6 Deve suportar expansão para portas 10G SFP+;

4.1.11.1.7 Deve suportar expansão para portas 40G QSFP+;

4.1.11.1.8 Possuir 1 interface de rede dedicada ao sincronismo;

4.1.11.1.9 Possuir 1 interface de rede dedicada ao gerenciamento;

4.1.11.1.10 Possuir 1 interface de rede dedicada para acesso via console;

4.1.11.1.11 Suportar até 225 (duzentos e vinte e cinco) instâncias (contextos) virtuais de firewall;

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

4.1.11.1.12.1 Por funcionalidades de proteção de rede e próxima geração entende-se: reconhecimento e controle granular de aplicações, prevenção de ameaças, identificação de usuários, IPS e Firewall;

4.1.11.1.13 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;

4.1.11.1.14 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;

4.1.11.1.15 Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19", incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;

4.1.11.2 **Funcionalidades Genéricas de Firewall**

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

4.1.11.2.1.1 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;

4.1.11.2.1.2 Deve suportar os seguintes tipos de NAT:

4.1.11.2.1.3 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;

4.1.11.2.1.4 Enviar logs para sistemas de monitoração externos, simultaneamente;

4.1.11.2.1.5 Prover mecanismo de prevenção a ataques de falsificação de endereços (IP Spoofing) através da especificação da interface de rede pela qual uma comunicação deverá se originar;

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

4.1.11.2.1.7 Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);

4.1.11.2.1.8 Suportar OSPF graceful restart;

4.1.11.2.1.9 Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

4.1.11.3 **Funcionalidades de Filtro de Conteúdo Web**

4.1.11.3.1 Controle de políticas por aplicações, grupos de aplicações e categorias de aplicações;

4.1.11.3.2 Controle de políticas por usuários, grupos de usuários, IPs e redes;

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

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

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

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

4.1.11.3.5.2 Reconhecer pelo menos 2.900 (duas mil e novecentas) 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;

4.1.11.3.6 A checagem de assinaturas deve determinar se uma aplicação está utilizando a porta padrão ou não;

4.1.11.3.7 Para tráfego criptografado (SSL), deve de-criptografar pacotes a fim de possibilitar a leitura do payload para checagem de assinaturas de aplicações conhecidas;

4.1.11.3.8 Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo;

4.1.11.3.9 A decodificação de protocolo deve também identificar comportamentos específicos dentro da aplicação;
4.1.11.3.10 Atualizar a base de assinaturas de aplicações automaticamente;
4.1.11.3.11 Limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD;
4.1.11.3.12 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;
4.1.11.3.13 Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos ou análise heurística;
4.1.11.3.14 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 banco;
4.1.11.3.15 Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;
4.1.11.3.16 A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:
4.1.11.3.16.1 Permitir especificar política por tempo, com definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
4.1.11.3.16.2 Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes;
4.1.11.3.16.3 Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs atráves da integração com serviços de diretório, autenticação via Active Directory e base de dados local;
4.1.11.3.16.4 Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;
4.1.11.3.16.5 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;
4.1.11.3.16.6 Suportar base ou cache de URLs local no appliance, evitando atrasos de comunicação e validação das URLs;
4.1.11.3.16.7 Suportar a criação de categorias de URLs customizadas;
4.1.11.3.16.8 Suportar a exclusão de URLs do bloqueio, por categoria;
4.1.11.3.16.9 Permitir a customização de página de bloqueio;
4.1.11.3.17 Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, sem a necessidade de instalar nenhum cliente nos servidores Active Directory ou em outra máquina da rede;
4.1.11.3.18 Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via Radius ou syslog, para a identificação de endereços IP e usuários;
4.1.11.3.19 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);

4.1.11.4 **Funcionalidade de Prevenção de Ameaças**
4.1.11.4.1 Os dispositivos de proteção devem possuir módulo de IPS e suportar os módulos de: Antivírus e Anti-Malware integrados no próprio equipamento;
4.1.11.4.2 Deve incluir assinaturas de prevenção de intrusão (IPS) e suporte ao bloqueio de arquivos maliciosos (Antivírus e Anti-Malware);
4.1.11.4.3 Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Malware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;
4.1.11.4.4 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;
4.1.11.4.5 Deverá possuir os seguintes mecanismos de inspeção de IPS:

4.1.11.4.5.1 Análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;
4.1.11.4.6 Detectar e bloquear a origem de portscans;
4.1.11.4.7 Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações;
4.1.11.4.8 Possuir assinaturas para bloqueio de ataques de buffer overflow;
4.1.11.4.9 Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP;
4.1.11.4.10 Suportar bloqueio de arquivos por tipo;
4.1.11.4.11 Identificar e bloquear comunicação com botnets;
4.1.11.4.12 Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:
4.1.11.4.12.1 O nome da assinatura e do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo de proteção;
4.1.11.4.13 Deve suportar a captura de pacotes (PCAP), em assinatura de IPS e Anti-Malware;
4.1.11.4.14 Os eventos devem identificar o país de onde partiu a ameaça;
4.1.11.4.15 Suportar rastreamento de vírus em arquivos pdf;
4.1.11.4.16 Deve suportar a inspeção em arquivos comprimidos (zip, gzip,etc.);
4.1.11.4.17 Suportar a criação de políticas por Geo Localização, permitindo que o tráfego de determinado País/Países seja bloqueado;
4.1.11.4.18 Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
4.1.11.4.19 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;

4.1.11.5 **Prevenção de Ameaças Avançadas**
4.1.11.5.1 A solução deverá prover as funcionalidades de inspeção e prevenção de tráfego de entrada de malwares não conhecidos e do tipo APT, com filtro de ameaças avançadas e análise de execução em tempo real e inspeção com prevenção de tráfego de saída de callbacks (comunicação do malware com o servidor de comando e controle);
4.1.11.5.2 Implementar, identificar e bloquear malwares de dia zero em anexos de e-mail e URL's conhecidas;
4.1.11.5.3 A solução deve fornecer a capacidade de emular ataques em diferentes sistemas operacionais, dentre eles: Windows XP (32 bits), Windows 7 (32 e 64 bits), Windows 8, Windows 8.1 e Windows 10 (64 bits), assim como Office 2003, 2010 e 2013;
4.1.11.5.4 Implementar gerenciamento SNMP v2 e v3;
4.1.11.5.5 Implementar mecanismo de exceção, permitindo a criação de regras por VLAN, subrede e endereço IP;
4.1.11.5.6 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: cab, csv, doc, docx, docm, dot, dotm, dotx, exe, hwp, jar, pdf, pif, ppam, pps, ppsm, ppsx, potx, potm, ppt, pptm, pptx, rar, rtf, seven-z, sldm, sldx, swf, tar, tgz, xlam, xls, xlsx, xlt, xltx, xlsm, xltm, xll, xlsb, zip;
4.1.11.5.7 Prover informações para que a solução de relatórios possa apresentar via interface gráfica as seguintes informações:
4.1.11.5.7.1 Sumário executivo;
4.1.11.5.7.2 Relatório de máquinas infectadas;
4.1.11.5.7.3 Atividades do malware durante a execução de arquivo, nos ambientes controlados em todas as versões de sistemas operacionais requisitados neste projeto;
4.1.11.5.8 A solução deve permitir a criação de whitelists baseado no MD5 do arquivo;
4.1.11.5.9 Para melhor administração da solução, a solução deve possibilitar as seguintes visualizações a nível de monitoração:
4.1.11.5.9.1 Número de arquivos emulados;

4.1.11.5.10 A solução de possuir os indicadores abaixo referente ao último dia, última semana ou últimos 30 dias:
4.1.11.5.10.1 Arquivos scaneados;
4.1.11.5.10.2 Arquivos maliciosos;

4.1.11.6 **Controle de Qualidade de Serviço**
4.1.11.6.1 Suportar a criação de políticas de QoS por:
4.1.11.6.1.1 Endereço de origem, endereço de destino e por porta;
4.1.11.6.2 O QoS deve possibilitar a definição de classes por:
4.1.11.6.2.1 Banda garantida, banda máxima e fila de prioridade;
4.1.11.6.2.2 Disponibilizar estatísticas RealTime para classes de QoS;

4.1.11.7 **Funcionalidades de VPN**
4.1.11.7.1 Suportar VPN Site-to-Site e Client-To-Site;
4.1.11.7.2 Suportar IPSec VPN;
4.1.11.7.3 Suportar SSL VPN;
4.1.11.7.4 A VPN IPSEc deve suportar:
4.1.11.7.4.1 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;
4.1.11.7.5 A VPN SSL deve suportar:
4.1.11.7.5.1 Permitir que o usuário realize a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;
4.1.11.7.5.2 A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;
4.1.11.7.5.3 Atribuição de endereço IP nos clientes remotos de VPN;
4.1.11.7.5.4 Atribuição de DNS nos clientes remotos de VPN;
4.1.11.7.5.5 Dever permitir criar políticas para tráfego dos clientes remotos conectados na VPN SSL;
4.1.11.7.5.6 Suportar autenticação via AD/LDAP, certificado digital e base de usuários local;
4.1.11.7.5.7 Suportar leitura e verificação de CRL (certificate revocation list);
4.1.11.7.5.8 O agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows XP, Vista, Windows 7, Windows 8 e MacOS X;

4.1.12 - **Item 07 -** Firewall – DATA CENTER TIPO III

4.1.12.1 **Características Gerais**
4.1.12.1.1 Throughput pelo menos de 23 Gbps, com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação e prevenção de ameaças avançadas habilitados simultaneamente;
4.1.12.1.1.1 O Throughput é considerado como a quantidade de tráfego que um único equipamento consegue redirecionar. Não há soma entre o tráfego de entrada e de saída das interfaces;
4.1.12.1.2 Suportar pelo menos 9.000.000 (nove milhões) de conexões ou sessões simultâneas;
4.1.12.1.3 Suportar pelo menos 540.000 (quinhentas e quarenta mil) novas conexões ou sessões por segundo;
4.1.12.1.4 Armazenamento interno em HDD ou SSD de pelo menos 480GB;
4.1.12.1.5 Possuir pelo menos 8 interfaces de rede 1GE UTP;
4.1.12.1.6 Deve suportar expansão para portas 10GE SFP+;
4.1.12.1.7 Deve suportar expansão para portas 40G QSFP+;
4.1.12.1.8 Possuir 1 interface de rede dedicada ao sincronismo;
4.1.12.1.9 Possuir 1 interface de rede dedicada ao gerenciamento;
4.1.12.1.10 Possuir 1 interface de rede dedicada para acesso via console;
4.1.12.1.11 Suportar até 225 (duzentos e vinte e cinco) instâncias (contextos) virtuais de firewall;

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

4.1.12.1.12.1 Por funcionalidades de proteção de rede e próxima geração entende-se: reconhecimento e controle granular de aplicações, prevenção de ameaças, identificação de usuários, IPS e Firewall;

4.1.12.1.13 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;

4.1.12.1.14 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;

4.1.12.1.15 Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19", incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;

4.1.12.2 **Funcionalidades Genéricas de Firewall**

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

4.1.12.2.1.1 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;

4.1.12.2.1.2 Deve suportar os seguintes tipos de NAT:

4.1.12.2.1.3 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;

4.1.12.2.1.4 Enviar logs para sistemas de monitoração externos, simultaneamente;

4.1.12.2.1.5 Prover mecanismo de prevenção a ataques de falsificação de endereços (IP Spoofing) através da especificação da interface de rede pela qual uma comunicação deverá se originar;

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

4.1.12.2.1.7 Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);

4.1.12.2.1.8 Suportar OSPF graceful restart;

4.1.12.2.1.9 Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

4.1.12.3 **Funcionalidades de Filtro de Conteúdo Web**

4.1.12.3.1 Controle de políticas por aplicações, grupos de aplicações e categorias de aplicações;

4.1.12.3.2 Controle de políticas por usuários, grupos de usuários, IPs e redes;

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

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

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

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

4.1.12.3.5.2 Reconhecer pelo menos 2.900 (duas mil e novecentas) 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;

4.1.12.3.6 A checagem de assinaturas deve determinar se uma aplicação está utilizando a porta padrão ou não;

4.1.12.3.7 Para tráfego criptografado (SSL), deve de-criptografar pacotes a fim de possibilitar a leitura do payload para checagem de assinaturas de aplicações conhecidas;

4.1.12.3.8 Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo;
4.1.12.3.9 A decodificação de protocolo deve também identificar comportamentos específicos dentro da aplicação;
4.1.12.3.10 Atualizar a base de assinaturas de aplicações automaticamente;
4.1.12.3.11 Limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD;
4.1.12.3.12 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;
4.1.12.3.13 Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos ou análise heurística;
4.1.12.3.14 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 banco;
4.1.12.3.15 Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;
4.1.12.3.16 A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:
4.1.12.3.16.1 Permitir especificar política por tempo, com definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
4.1.12.3.16.2 Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes;
4.1.12.3.16.3 Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs atráves da integração com serviços de diretório, autenticação via Active Directory e base de dados local;
4.1.12.3.16.4 Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;
4.1.12.3.16.5 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;
4.1.12.3.16.6 Suportar base ou cache de URLs local no appliance, evitando atrasos de comunicação e validação das URLs;
4.1.12.3.16.7 Suportar a criação de categorias de URLs customizadas;
4.1.12.3.16.8 Suportar a exclusão de URLs do bloqueio, por categoria;
4.1.12.3.16.9 Permitir a customização de página de bloqueio;
4.1.12.3.17 Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, sem a necessidade de instalar nenhum cliente nos servidores Active Directory ou em outra máquina da rede;
4.1.12.3.18 Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via Radius ou syslog, para a identificação de endereços IP e usuários;
4.1.12.3.19 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);

4.1.12.4 **Funcionalidade de Prevenção de Ameaças**
4.1.12.4.1 Os dispositivos de proteção devem possuir módulo de IPS e suportar os módulos de: Antivírus e Anti-Malware integrados no próprio equipamento;
4.1.12.4.2 Deve incluir assinaturas de prevenção de intrusão (IPS) e suporte ao bloqueio de arquivos maliciosos (Antivírus e Anti-Malware);
4.1.12.4.3 Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Malware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;
4.1.12.4.4 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;

4.1.12.4.5 Deverá possuir os seguintes mecanismos de inspeção de IPS:
4.1.12.4.5.1 Análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;
4.1.12.4.6 Detectar e bloquear a origem de portscans;
4.1.12.4.7 Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações;
4.1.12.4.8 Possuir assinaturas para bloqueio de ataques de buffer overflow;
4.1.12.4.9 Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP;
4.1.12.4.10 Suportar bloqueio de arquivos por tipo;
4.1.12.4.11 Identificar e bloquear comunicação com botnets;
4.1.12.4.12 Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:
4.1.12.4.12.1 O nome da assinatura e do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo de proteção;
4.1.12.4.13 Deve suportar a captura de pacotes (PCAP), em assinatura de IPS e Anti-Malware;
4.1.12.4.14 Os eventos devem identificar o país de onde partiu a ameaça;
4.1.12.4.15 Suportar rastreamento de vírus em arquivos pdf;
4.1.12.4.16 Deve suportar a inspeção em arquivos comprimidos (zip, gzip,etc.);
4.1.12.4.17 Suportar a criação de políticas por Geo Localização, permitindo que o tráfego de determinado País/Países seja bloqueado;
4.1.12.4.18 Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
4.1.12.4.19 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;

4.1.12.5 **Prevenção de Ameaças Avançadas**
4.1.12.5.1 A solução deverá prover as funcionalidades de inspeção e prevenção de tráfego de entrada de malwares não conhecidos e do tipo APT, com filtro de ameaças avançadas e análise de execução em tempo real e inspeção com prevenção de tráfego de saída de callbacks (comunicação do malware com o servidor de comando e controle);
4.1.12.5.2 Implementar, identificar e bloquear malwares de dia zero em anexos de e-mail e URL's conhecidas;
4.1.12.5.3 A solução deve fornecer a capacidade de emular ataques em diferentes sistemas operacionais, dentre eles: Windows XP (32 bits), Windows 7 (32 e 64 bits), Windows 8, Windows 8.1 e Windows 10 (64 bits), assim como Office 2003, 2010 e 2013;
4.1.12.5.4 Implementar gerenciamento SNMP v2 e v3;
4.1.12.5.5 Implementar mecanismo de exceção, permitindo a criação de regras por VLAN, subrede e endereço IP;
4.1.12.5.6 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: cab, csv, doc, docx, docm, dot, dotm, dotx, exe, hwp, jar, pdf, pif, ppam, pps, ppsm, ppsx, potx, potm, ppt, pptm, pptx, rar, rtf, seven-z, sldm, sldx, swf, tar, tgz, xlam, xls, xlsx, xlt, xltx, xlsm, xltm, xll, xlsb, zip;
4.1.12.5.7 Prover informações para que a solução de relatórios possa apresentar via interface gráfica as seguintes informações:
4.1.12.5.7.1 Sumário executivo;
4.1.12.5.7.2 Relatório de máquinas infectadas;
4.1.12.5.7.3 Atividades do malware durante a execução de arquivo, nos ambientes controlados em todas as versões de sistemas operacionais requisitados neste projeto;
4.1.12.5.8 A solução deve permitir a criação de whitelists baseado no MD5 do arquivo;
4.1.12.5.9 Para melhor administração da solução, a solução deve possibilitar as seguintes visualizações a nível de monitoração:
4.1.12.5.9.1 Número de arquivos emulados;

4.1.12.5.10 A solução de possuir os indicadores abaixo referente ao último dia, última semana ou últimos 30 dias:
4.1.12.5.10.1 Arquivos scaneados;
4.1.12.5.10.2 Arquivos maliciosos;

4.1.12.6 **Controle de Qualidade de Serviço**
4.1.12.6.1 Suportar a criação de políticas de QoS por:
4.1.12.6.1.1 Endereço de origem, endereço de destino e por porta;
4.1.12.6.2 O QoS deve possibilitar a definição de classes por:
4.1.12.6.2.1 Banda garantida, banda máxima e fila de prioridade;
4.1.12.6.2.2 Disponibilizar estatísticas RealTime para classes de QoS;

4.1.12.7 **Funcionalidades de VPN**
4.1.12.7.1 Suportar VPN Site-to-Site e Client-To-Site;
4.1.12.7.2 Suportar IPSec VPN;
4.1.12.7.3 Suportar SSL VPN;
4.1.12.7.4 A VPN IPSEc deve suportar:
4.1.12.7.4.1 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;
4.1.12.7.5 A VPN SSL deve suportar:
4.1.12.7.5.1 Permitir que o usuário realize a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;
4.1.12.7.5.2 A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;
4.1.12.7.5.3 Atribuição de endereço IP nos clientes remotos de VPN;
4.1.12.7.5.4 Atribuição de DNS nos clientes remotos de VPN;
4.1.12.7.5.5 Dever permitir criar políticas para tráfego dos clientes remotos conectados na VPN SSL;
4.1.12.7.5.6 Suportar autenticação via AD/LDAP, certificado digital e base de usuários local;
4.1.12.7.5.7 Suportar leitura e verificação de CRL (certificate revocation list);
4.1.12.7.5.8 O agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows XP, Vista, Windows 7, Windows 8 e MacOS X;

4.1.13 - **Item 08 -** Firewall para Nuvem Privada

4.1.13.1 **Características Gerais**
4.1.13.1.1 O licenciamento deverá ser feito pelo número de cores virtuais;
4.1.13.1.2 Deve ser compatível com, pelo menos, os seguintes hypervisors: VMware ESXi, Microsoft Hyper-V e KVM;
4.1.13.1.3 A solução deverá permitir expansão através de adição de novas licenças, de forma que suporte à criação de "pools" de gateways virtuais;
4.1.13.1.4 A solução para ambientes virtualizados deve suportar os seguintes SDN de mercado para integração: OpenStack, Cisco ACI, VMware NSX, e ESXi.

4.1.13.2 **Funcionalidades Genéricas de Firewall**
4.1.13.2.1 Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:
4.1.13.2.1.1 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;
4.1.13.2.1.2 **Deve suportar os seguintes tipos de NAT:**

4.1.13.2.1.3 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;

4.1.13.2.1.4 Enviar logs para sistemas de monitoração externos, simultaneamente;

4.1.13.2.1.5 Prover mecanismo de prevenção a ataques de falsificação de endereços (IP Spoofing) através da especificação da interface de rede pela qual uma comunicação deverá se originar;

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

4.1.13.2.1.7 Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);

4.1.13.2.1.8 Suportar OSPF graceful restart;

4.1.13.2.1.9 Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

4.1.13.3 **Funcionalidades de Filtro de Conteúdo Web**

4.1.13.3.1 Controle de políticas por aplicações, grupos de aplicações e categorias de aplicações;

4.1.13.3.2 Controle de políticas por usuários, grupos de usuários, IPs e redes;

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

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

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

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

4.1.13.3.5.2 Reconhecer pelo menos 2.900 (duas mil e novecentas) 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;

4.1.13.3.6 A checagem de assinaturas deve determinar se uma aplicação está utilizando a porta padrão ou não;

4.1.13.3.7 Para tráfego criptografado (SSL), deve de-criptografar pacotes a fim de possibilitar a leitura do payload para checagem de assinaturas de aplicações conhecidas;

4.1.13.3.8 Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo;

4.1.13.3.9 A decodificação de protocolo deve também identificar comportamentos específicos dentro da aplicação;

4.1.13.3.10 Atualizar a base de assinaturas de aplicações automaticamente;

4.1.13.3.11 Limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD;

4.1.13.3.12 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;

4.1.13.3.13 Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos ou análise heurística;

4.1.13.3.14 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 banco;

4.1.13.3.15 Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;

4.1.13.3.16 A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:

4.1.13.3.16.1 Permitir especificar política por tempo, com definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

4.1.13.3.16.2 Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes;

4.1.13.3.16.3 Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs atráves da integração com serviços de diretório, autenticação via Active Directory e base de dados local;

4.1.13.3.16.4 Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;
4.1.13.3.16.5 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;
4.1.13.3.16.6 Suportar base ou cache de URLs local no appliance, evitando atrasos de comunicação e validação das URLs;
4.1.13.3.16.7 Suportar a criação de categorias de URLs customizadas;
4.1.13.3.16.8 Suportar a exclusão de URLs do bloqueio, por categoria;
4.1.13.3.16.9 Permitir a customização de página de bloqueio;
4.1.13.3.17 Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, sem a necessidade de instalar nenhum cliente nos servidores Active Directory ou em outra máquina da rede;
4.1.13.3.18 Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via Radius ou syslog, para a identificação de endereços IP e usuários;
4.1.13.3.19 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);

4.1.13.4 **Funcionalidade de Prevenção de Ameaças**
4.1.13.4.1 Os dispositivos de proteção devem possuir módulo de IPS e suportar os módulos de: Antivírus e Anti-Malware integrados no próprio equipamento;
4.1.13.4.2 Deve incluir assinaturas de prevenção de intrusão (IPS) e suporte ao bloqueio de arquivos maliciosos (Antivírus e Anti-Malware);
4.1.13.4.3 Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Malware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;
4.1.13.4.4 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;
4.1.13.4.5 Deverá possuir os seguintes mecanismos de inspeção de IPS:
4.1.13.4.5.1 Análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;
4.1.13.4.6 Detectar e bloquear a origem de portscans;
4.1.13.4.7 Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações;
4.1.13.4.8 Possuir assinaturas para bloqueio de ataques de buffer overflow;
4.1.13.4.9 Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP;
4.1.13.4.10 Suportar bloqueio de arquivos por tipo;
4.1.13.4.11 Identificar e bloquear comunicação com botnets;
4.1.13.4.12 Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:
4.1.13.4.12.1 O nome da assinatura e do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo de proteção;
4.1.13.4.13 Deve suportar a captura de pacotes (PCAP), em assinatura de IPS e Anti-Malware;
4.1.13.4.14 Os eventos devem identificar o país de onde partiu a ameaça;
4.1.13.4.15 Suportar rastreamento de vírus em arquivos pdf;
4.1.13.4.16 Deve suportar a inspeção em arquivos comprimidos (zip, gzip,etc.);
4.1.13.4.17 Suportar a criação de políticas por Geo Localização, permitindo que o tráfego de determinado País/Países seja bloqueado;
4.1.13.4.18 Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

4.1.13.4.19 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;

4.1.13.5 **Prevenção de Ameaças Avançadas**

4.1.13.5.1 A solução deverá prover as funcionalidades de inspeção e prevenção de tráfego de entrada de malwares não conhecidos e do tipo APT, com filtro de ameaças avançadas e análise de execução em tempo real e inspeção com prevenção de tráfego de saída de callbacks (comunicação do malware com o servidor de comando e controle);

4.1.13.5.2 Implementar, identificar e bloquear malwares de dia zero em anexos de e-mail e URL's conhecidas;

4.1.13.5.3 A solução deve fornecer a capacidade de emular ataques em diferentes sistemas operacionais, dentre eles: Windows XP (32 bits), Windows 7 (32 e 64 bits), Windows 8, Windows 8.1 e Windows 10 (64 bits), assim como Office 2003, 2010 e 2013;

4.1.13.5.4 Implementar gerenciamento SNMP v2 e v3;

4.1.13.5.5 Implementar mecanismo de exceção, permitindo a criação de regras por VLAN, subrede e endereço IP;

4.1.13.5.6 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: cab, csv, doc, docx, docm, dot, dotm, dotx, exe, hwp, jar, pdf, pif, ppam, pps, ppsm, ppsx, potx, potm, ppt, pptm, pptx, rar, rtf, seven-z, sldm, sldx, swf, tar, tgz, xlam, xls, xlsx, xlt, xltx, xlsm, xltm, xll, xlsb, zip;

4.1.13.5.7 Prover informações para que a solução de relatórios possa apresentar via interface gráfica as seguintes informações:

4.1.13.5.7.1 Sumário executivo;

4.1.13.5.7.2 Relatório de máquinas infectadas;

4.1.13.5.7.3 Atividades do malware durante a execução de arquivo, nos ambientes controlados em todas as versões de sistemas operacionais requisitados neste projeto;

4.1.13.5.8 A solução deve permitir a criação de whitelists baseado no MD5 do arquivo;

4.1.13.5.9 Para melhor administração da solução, a solução deve possibilitar as seguintes visualizações a nível de monitoração:

4.1.13.5.9.1 Número de arquivos emulados;

4.1.13.5.10 A solução de possuir os indicadores abaixo referente ao último dia, última semana ou últimos 30 dias:

4.1.13.5.10.1 Arquivos scaneados;

4.1.13.5.10.2 Arquivos maliciosos;

4.1.13.6 **Controle de Qualidade de Serviço**

4.1.13.6.1 Suportar a criação de políticas de QoS por:

4.1.13.6.1.1 Endereço de origem, endereço de destino e por porta;

4.1.13.6.2 O QoS deve possibilitar a definição de classes por:

4.1.13.6.2.1 Banda garantida, banda máxima e fila de prioridade;

4.1.13.6.2.2 Disponibilizar estatísticas RealTime para classes de QoS;

4.1.13.7 **Funcionalidades de VPN**

4.1.13.7.1 Suportar VPN Site-to-Site e Client-To-Site;

4.1.13.7.2 Suportar IPSec VPN;

4.1.13.7.3 Suportar SSL VPN;

4.1.13.7.4 A VPN IPSEc deve suportar:

4.1.13.7.4.1 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;

4.1.13.7.5 **A VPN SSL deve suportar:**

4.1.13.7.5.1 Permitir que o usuário realize a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;
4.1.13.7.5.2 A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;
4.1.13.7.5.3 Atribuição de endereço IP nos clientes remotos de VPN;
4.1.13.7.5.4 Atribuição de DNS nos clientes remotos de VPN;
4.1.13.7.5.5 Dever permitir criar políticas para tráfego dos clientes remotos conectados na VPN SSL;
4.1.13.7.5.6 Suportar autenticação via AD/LDAP, certificado digital e base de usuários local;
4.1.13.7.5.7 Suportar leitura e verificação de CRL (certificate revocation list);
4.1.13.7.5.8 O agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows XP, Vista, Windows 7, Windows 8 e MacOS X;

4.1.14 - **Item 09 -** Firewall para Nuvem Pública

4.1.14.1 **Características Gerais**
4.1.14.1.1 A solução deve estar listada como parceiro de segurança em pelo menos dois provedores de nuvens entre AWS, Azure, IBM, Mandic e Oracle;
4.1.14.1.2 A solução dever fazer parte do market place de pelo menos dois provedores de nuvens entre AWS, Azure, IBM, Mandic e Oracle;
4.1.14.1.3 A solução deve possuir, pelo menos, os métodos de licenciamento *"pay as you go"* e *"bring your own license"*
4.1.14.1.4 A solução deve suportar políticas de segurança dinâmicas que utilizem os objetos definidos no provedor de nuvem ajustando automaticamente a segurança com as mudanças que ocorrem num ambiente dinâmico de nuvem.
4.1.14.1.5 Deve ser capaz de utilizar objetos de pelo menos dois provedores de nuvens entre AWS, Azure, IBM, Mandic e Oracle, nas políticas de segurança;
4.1.14.1.6 Deve ser capaz de receber atualizações automáticas de objetos localizados, de pelo menos dois provedores de nuvens entre AWS, Azure, IBM, Mandic e Oracle, sem a necessidade de alterar a política;

4.1.14.2 **Funcionalidades Genéricas de Firewall**
4.1.14.2.1 Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:
4.1.14.2.1.1 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;
4.1.14.2.1.2 Deve suportar os seguintes tipos de NAT:
4.1.14.2.1.3 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;
4.1.14.2.1.4 Enviar logs para sistemas de monitoração externos, simultaneamente;
4.1.14.2.1.5 Prover mecanismo de prevenção a ataques de falsificação de endereços (IP Spoofing) através da especificação da interface de rede pela qual uma comunicação deverá se originar;
4.1.14.2.1.6 Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
4.1.14.2.1.7 Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);
4.1.14.2.1.8 Suportar OSPF graceful restart;
4.1.14.2.1.9 Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

4.1.14.3 **Funcionalidades de Filtro de Conteúdo Web**
4.1.14.3.1 Controle de políticas por aplicações, grupos de aplicações e categorias de aplicações;
4.1.14.3.2 Controle de políticas por usuários, grupos de usuários, IPs e redes;

4.1.14.3.3 Deve de-criptografar tráfego de entrada e saída em conexões negociadas com TLS 1.2;
4.1.14.3.4 Suportar a atribuição de agendamento às políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;
4.1.14.3.5 Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:
4.1.14.3.5.1 Deve ser possível a liberação e bloqueio de aplicações sem a necessidade de liberação de portas e protocolos;
4.1.14.3.5.2 Reconhecer pelo menos 2.900 (duas mil e novecentas) 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;
4.1.14.3.6 A checagem de assinaturas deve determinar se uma aplicação está utilizando a porta padrão ou não;
4.1.14.3.7 Para tráfego criptografado (SSL), deve de-criptografar pacotes a fim de possibilitar a leitura do payload para checagem de assinaturas de aplicações conhecidas;
4.1.14.3.8 Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo;
4.1.14.3.9 A decodificação de protocolo deve também identificar comportamentos específicos dentro da aplicação;
4.1.14.3.10 Atualizar a base de assinaturas de aplicações automaticamente;
4.1.14.3.11 Limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD;
4.1.14.3.12 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;
4.1.14.3.13 Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos ou análise heurística;
4.1.14.3.14 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 banco;
4.1.14.3.15 Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;
4.1.14.3.16 A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:
4.1.14.3.16.1 Permitir especificar política por tempo, com definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
4.1.14.3.16.2 Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes;
4.1.14.3.16.3 Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs atráves da integração com serviços de diretório, autenticação via Active Directory e base de dados local;
4.1.14.3.16.4 Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;
4.1.14.3.16.5 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;
4.1.14.3.16.6 Suportar base ou cache de URLs local no appliance, evitando atrasos de comunicação e validação das URLs;
4.1.14.3.16.7 Suportar a criação de categorias de URLs customizadas;
4.1.14.3.16.8 Suportar a exclusão de URLs do bloqueio, por categoria;
4.1.14.3.16.9 Permitir a customização de página de bloqueio;
4.1.14.3.17 Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, sem a necessidade de instalar nenhum cliente nos servidores Active Directory ou em outra máquina da rede;

4.1.14.3.18 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);

4.1.14.4 **Funcionalidade de Prevenção de Ameaças**

4.1.14.4.1 Os dispositivos de proteção devem possuir módulo de IPS e suportar os módulos de: Antivírus e Anti-Malware integrados no próprio equipamento;

4.1.14.4.2 Deve incluir assinaturas de prevenção de intrusão (IPS) e suporte ao bloqueio de arquivos maliciosos (Antivírus e Anti-Malware);

4.1.14.4.3 Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Malware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;

4.1.14.4.4 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;

4.1.14.4.5 Deverá possuir os seguintes mecanismos de inspeção de IPS:

4.1.14.4.5.1 Análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;

4.1.14.4.6 Detectar e bloquear a origem de portscans;

4.1.14.4.7 Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações;

4.1.14.4.8 Possuir assinaturas para bloqueio de ataques de buffer overflow;

4.1.14.4.9 Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP;

4.1.14.4.10 Suportar bloqueio de arquivos por tipo;

4.1.14.4.11 Identificar e bloquear comunicação com botnets;

4.1.14.4.12 Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:

4.1.14.4.12.1 O nome da assinatura e do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo de proteção;

4.1.14.4.13 Deve suportar a captura de pacotes (PCAP), em assinatura de IPS e Anti-Malware;

4.1.14.4.14 Os eventos devem identificar o país de onde partiu a ameaça;

4.1.14.4.15 Suportar rastreamento de vírus em arquivos pdf;

4.1.14.4.16 Deve suportar a inspeção em arquivos comprimidos (zip, gzip,etc.);

4.1.14.4.17 Suportar a criação de políticas por Geo Localização, permitindo que o tráfego de determinado País/Países seja bloqueado;

4.1.14.4.18 Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

4.1.14.4.19 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;

4.1.14.5 **Prevenção de Ameaças Avançadas**

4.1.14.5.1 A solução deverá prover as funcionalidades de inspeção e prevenção de tráfego de entrada de malwares não conhecidos e do tipo APT, com filtro de ameaças avançadas e análise de execução em tempo real e inspeção com prevenção de tráfego de saída de callbacks (comunicação do malware com o servidor de comando e controle);

4.1.14.5.2 Implementar, identificar e bloquear malwares de dia zero em anexos de e-mail e URL's conhecidas;

4.1.14.5.3 A solução deve fornecer a capacidade de emular ataques em diferentes sistemas operacionais, dentre eles: Windows XP (32 bits), Windows 7 (32 e 64 bits), Windows 8, Windows 8.1 e Windows 10 (64 bits), assim como Office 2003, 2010 e 2013;

4.1.14.5.4 Implementar gerenciamento SNMP v2 e v3;

4.1.14.5.5 Implementar mecanismo de exceção, permitindo a criação de regras por VLAN, subrede e endereço IP;

4.1.14.5.6 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: cab, csv, doc, docx, docm, dot, dotm, dotx, exe, hwp, jar, pdf, pif, ppam, pps, ppsm, ppsx, potx, potm, ppt, pptm, pptx, rar, rtf, seven-z, sldm, sldx, swf, tar, tgz, xlam, xls, xlsx, xlt, xltx, xlsm, xltm, xll, xlsb, zip;

4.1.14.5.7 Prover informações para que a solução de relatórios possa apresentar via interface gráfica as seguintes informações:

4.1.14.5.7.1 Sumário executivo;

4.1.14.5.7.2 Relatório de máquinas infectadas;

4.1.14.5.7.3 Atividades do malware durante a execução de arquivo, nos ambientes controlados em todas as versões de sistemas operacionais requisitados neste projeto;

4.1.14.5.8 A solução deve permitir a criação de whitelists baseado no MD5 do arquivo;

4.1.14.5.9 Para melhor administração da solução, a solução deve possibilitar as seguintes visualizações a nível de monitoração:

4.1.14.5.9.1 Número de arquivos emulados;

4.1.14.5.10 A solução de possuir os indicadores abaixo referente ao último dia, última semana ou últimos 30 dias:

4.1.14.5.10.1 Arquivos scaneados;

4.1.14.5.10.2 Arquivos maliciosos;

4.1.14.6 **Controle de Qualidade de Serviço**

4.1.14.6.1 Suportar a criação de políticas de QoS por:

4.1.14.6.1.1 Endereço de origem, endereço de destino e por porta;

4.1.14.6.2 O QoS deve possibilitar a definição de classes por:

4.1.14.6.2.1 Banda garantida, banda máxima e fila de prioridade;

4.1.14.6.2.2 Disponibilizar estatísticas RealTime para classes de QoS;

4.1.14.7 **Funcionalidades de VPN**

4.1.14.7.1 Suportar VPN Site-to-Site e Client-To-Site;

4.1.14.7.2 Suportar IPSec VPN;

4.1.14.7.3 Suportar SSL VPN;

4.1.14.7.4 A VPN IPSEc deve suportar:

4.1.14.7.4.1 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;

4.1.14.7.5 A VPN SSL deve suportar:

4.1.14.7.5.1 Permitir que o usuário realize a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;

4.1.14.7.5.2 A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;

4.1.14.7.5.3 Atribuição de endereço IP nos clientes remotos de VPN;

4.1.14.7.5.4 Atribuição de DNS nos clientes remotos de VPN;

4.1.14.7.5.5 Dever permitir criar políticas para tráfego dos clientes remotos conectados na VPN SSL;

4.1.14.7.5.6 Suportar autenticação via AD/LDAP, certificado digital e base de usuários local;

4.1.14.7.5.7 Suportar leitura e verificação de CRL (certificate revocation list);

4.1.14.7.5.8 O agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows XP, Vista, Windows 7, Windows 8 e MacOS X;

4.1.15 - **Item 10 -** Solução de Segurança e Visibilidade para Ambientes Multi-Cloud

4.1.15.1 **Características Gerais**

4.1.15.1.1 Deve suportar ambientes multi-cloud, incluindo pelo menos dois provedores de nuvens entre AWS, Azure, IBM, Mandic e Oracle.

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

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

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

4.1.15.1.5 A solução deverá realizar coleta automatizada de informações dos ambientes de pelo menos dois provedores de nuvens entre AWS, Azure, IBM, Mandic e Oracle, sem a necessidade de agentes e classificar de forma automática os assets protegidos com base no nível de exposição ao mundo exterior (internet).

4.1.15.1.6 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.

4.1.15.1.7 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.)

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

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

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

4.1.15.1.11 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).

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

4.1.15.1.13 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.

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

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

4.1.15.1.16 Deverá correlacionar conjuntos de dados para identificar aplicativos

4.1.15.1.17 Deverá correlacionar conjuntos de dados para criar mapeamento de fluxo

4.1.15.1.18 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.

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

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

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

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

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

4.1.16 **Item 11 -** Firewall – UNIDADE REMOTA TIPO I

4.1.16.1 **Características Gerais**

4.1.16.1.1 Throughput de pelo menos 220 Mbps, com as funcionalidades de firewall, prevenção de intrusão e controle de aplicação habilitados simultaneamente;

4.1.16.1.1.1 O Throughput é considerado como a quantidade de tráfego que um único equipamento consegue redirecionar. Não há soma entre o tráfego de entrada e de saída das interfaces;

4.1.16.1.2 Suportar pelo menos 495.000 (quatrocentas e noventa e cinco mil) conexões ou sessões simultâneas;

4.1.16.1.3 Suportar pelo menos 19.000 (dezenove mil) novas conexões ou sessões por segundo;

4.1.16.1.4 Throughput de 270 Mbps para VPN;

4.1.16.1.5 Possuir pelo menos 8 interfaces de rede 1G UTP;

4.1.16.2 **Funcionalidades Genéricas de Firewall**

4.1.16.2.1 Deve suportar autenticação para o serviço NTP.

4.1.16.2.2 Deve ser possível definir por quais origens são permitidas as conexões do administrador. Por exemplo: LAN, Rede Wireless Confiável, VPN, Internet etc.

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

4.1.16.2.4 Deve suportar SNMP v2 e v3.

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

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

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

4.1.16.2.8 Deve ser possível conectar a serviços de DDNS;

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

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

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

4.1.16.2.12 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;

4.1.16.2.13 A solução deve identificar usuários das seguintes fontes pelo menos:

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

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

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

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

4.1.16.3 **Funcionalidade de Prevenção de Ameaças**

4.1.16.3.1 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.

4.1.16.3.2 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;

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

4.1.16.3.4 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;

4.1.16.3.5 Deve ser capaz de bloquear tráfego SSH em DNS tunneling;
4.1.16.3.6 A solução deverá ser capaz de inspecionar e proteger apenas hosts internos ou inspecionar todo o tráfego;
4.1.16.3.7 A solução deve proteger contra ataques do tipo envenenamento de cache DNS (DNS Cache Poisoning);
4.1.16.3.8 A solução deverá possuir pelo menos dois perfis pré-configurados de fábrica para uso imediato e permitir a customização de um perfil;
4.1.16.3.9 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;
4.1.16.3.10 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;
4.1.16.3.11 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.

4.1.16.3.12 Deve ser possível visualizar a lista de proteções disponíveis no equipamento com os detalhes.
4.1.16.3.13 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).
4.1.16.3.14 A solução deve bloquear arquivos potencialmente maliciosos infectados com malware.
4.1.16.3.15 A solução de proteção contra malware e bot deve compartilhar a mesma política para facilitar o gerenciamento.
4.1.16.3.16 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;
4.1.16.3.17 As proteções devem ser ativadas baseadas em, pelo menos, critério de nível de confiança, ações da proteção e impacto de performance.
4.1.16.3.18 Deve ser possível habilitar a trilha das proteções para não logar, criar um log ou gerar um alerta;
4.1.16.3.19 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.

4.1.16.3.20 A solução de anti-malware deve suportar protocolos SMTP e POP3, FTP, HTTP em qualquer porta;
4.1.16.3.21 Deve ser possível definir uma política de inspeção para os tipos de arquivos por:
4.1.16.3.21.1 Inspecionar tipos de arquivos conhecidos que contenham malware;
4.1.16.3.21.2 Inspecionar todos os tipos de arquivos;
4.1.16.3.21.3 Inspecionar tipos de arquivos de famílias específicas;
4.1.16.3.21.4 Deve bloquear acesso a URLs com malware;
4.1.16.3.22 Deve ser possível customizar a página exibida para o usuário quando a URL contiver um malware e o acesso for bloqueado;

4.1.16.4 **Filtro de Conteúdo Web**
4.1.16.4.1 A solução deverá contar com ferramentas de visibilidade e controle de aplicações web e filtro URL integrada no próprio appliance de segurança que permita a criação de políticas de liberação ou bloqueio baseando-se em aplicações web e URL;
4.1.16.4.2 A gerência das políticas de segurança de controle de aplicação e controle de URL's deverá ser realizada na mesma interface web de gerenciamento;
4.1.16.4.3 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.
4.1.16.4.4 Deve ser possível configurar com apenas um clique o bloqueio a sites com conteúdo inapropriado como sexo, violência, armas, jogos e álcool.
4.1.16.4.5 Deve configurar regras para permitir ou bloquear aplicações ou páginas da Internet por pelo menos:

4.1.16.4.5.1 Usuário do Active Directory
4.1.16.4.5.2 IP
4.1.16.4.5.3 Rede
4.1.16.4.6 Deve ser possível configurar o bloqueio de compartilhamento de arquivos com origem usualmente ilegais como aplicações torrents e peer-to-peer.
4.1.16.4.7 Deve ser possível configurar manualmente o bloqueio de aplicações ou categorias de sites de aplicações indesejadas.
4.1.16.4.8 Deve ainda ser possível adicionar uma URL ou aplicação que não está na base de dados.
4.1.16.4.9 Deve ser possível limitar o consumo de banda de aplicações.
4.1.16.4.10 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;
4.1.16.4.11 Deve ser possível realizar a recategorização de uma URL através da gerência do equipamento.
4.1.16.4.12 Deve ser possível customizar e definir a frequência com que serão exibidas as mensagens para os usuários nas seguintes ações:
4.1.16.4.12.1 Aceitar e informar
4.1.16.4.12.2 Bloquear e informar
4.1.16.4.12.3 Perguntar

4.1.16.5 **Acesso Remoto**
4.1.16.5.1 A solução deve prover acesso seguro encriptado aos usuários remotos através da Internet;
4.1.16.5.2 A solução deve prover conectividade através de um cliente instalado no computador do usuário e através do navegador do usuário com conexão segura (HTTPS).
4.1.16.5.3 Deve suportar pelo menos os seguintes métodos de conexão:
4.1.16.5.3.1 Conexão através de cliente instalado no laptop ou desktop do usuário.
4.1.16.5.3.2 Conexão através de cliente instalado no smartphone e tablets.
4.1.16.5.3.3 Conexão através de navegador com SSL.
4.1.16.5.3.4 Conexão através de cliente nativo Windows L2TP.
4.1.16.5.4 Solução deve suportar alterar a porta padrão 443 para estabelecimento de VPN SSL.
4.1.16.5.5 A solução deve permitir conexão VPN aos seguintes usuários:
4.1.16.5.5.1 Usuários locais na própria base do appliance.
4.1.16.5.5.2 Grupos de usuários locais na própria base do appliance.
4.1.16.5.5.3 Grupos de usuários do Active Directory.
4.1.16.5.5.4 Grupos de usuários Radius.
4.1.16.5.6 A solução deve permitir atribuir um endereço específico para o usuário remoto.

4.1.16.6 **Funcionalidade de VPN Site-to-Site**
4.1.16.6.1 A solução deve prover acesso seguro criptografado entre duas localidades através da Internet;
4.1.16.6.2 A solução deve estabelecer VPN com o site remoto do próprio fabricante ou de terceiros;
4.1.16.6.3 A solução deve suportar autenticação com senha ou certificado;
4.1.16.6.4 Deve suportar, pelo menos, criptografia AES 128 e 256;
4.1.16.6.5 Deve possuir mecanismo para monitorar a saúde do túnel remoto;
4.1.16.6.6 Quando o túnel for estabelecido entre dispositivos do mesmo fabricante este deve possuir protocolo proprietário para testar se o túnel está ativo.

4.1.17 **Item 12 -** Firewall – UNIDADE REMOTA TIPO II

4.1.17.1 **Características Gerais**
4.1.17.1.1 Throughput de pelo menos 495 Mbps, com as funcionalidades de firewall, prevenção de intrusão e controle de aplicação habilitados simultaneamente;

4.1.17.1.1.1 O Throughput é considerado como a quantidade de tráfego que um único equipamento consegue redirecionar. Não há soma entre o tráfego de entrada e de saída das interfaces;

4.1.17.1.2 Suportar pelo menos 495.000 (quatrocentas e noventa e cinco mil) conexões ou sessões simultâneas;

4.1.17.1.3 Suportar pelo menos 29.000 (vinte e nove mil) novas conexões ou sessões por segundo;

4.1.17.1.4 Throughput de 495 Mbps para VPN;

4.1.17.1.5 Possuir pelo menos 16 interfaces de rede 1G UTP;

4.1.17.2 **Funcionalidades Genéricas de Firewall**

4.1.17.2.1 Deve suportar autenticação para o serviço NTP.

4.1.17.2.2 Deve ser possível definir por quais origens são permitidas as conexões do administrador. Por exemplo: LAN, Rede Wireless Confiável, VPN, Internet etc.

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

4.1.17.2.4 Deve suportar SNMP v2 e v3.

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

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

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

4.1.17.2.8 Deve ser possível conectar a serviços de DDNS;

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

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

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

4.1.17.2.12 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;

4.1.17.2.13 A solução deve identificar usuários das seguintes fontes pelo menos:

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

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

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

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

4.1.17.3 **Funcionalidade de Prevenção de Ameaças**

4.1.17.3.1 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.

4.1.17.3.2 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;

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

4.1.17.3.4 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;

4.1.17.3.5 Deve ser capaz de bloquear tráfego SSH em DNS tunneling;

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

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

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

4.1.17.3.9 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;

4.1.17.3.10 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;

4.1.17.3.11 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.

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

4.1.17.3.13 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).

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

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

4.1.17.3.16 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;

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

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

4.1.17.3.19 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.

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

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

4.1.17.3.21.1 Inspecionar tipos de arquivos conhecidos que contenham malware;

4.1.17.3.21.2 Inspecionar todos os tipos de arquivos;

4.1.17.3.21.3 Inspecionar tipos de arquivos de famílias específicas;

4.1.17.3.21.4 Deve bloquear acesso a URLs com malware;

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

4.1.17.4 **Filtro de Conteúdo Web**

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

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

4.1.17.4.3 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.

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

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

4.1.17.4.5.1 Usuário do Active Directory

4.1.17.4.5.2 IP
4.1.17.4.5.3 Rede
4.1.17.4.6 Deve ser possível configurar o bloqueio de compartilhamento de arquivos com origem usualmente ilegais como aplicações torrents e peer-to-peer.
4.1.17.4.7 Deve ser possível configurar manualmente o bloqueio de aplicações ou categorias de sites de aplicações indesejadas.
4.1.17.4.8 Deve ainda ser possível adicionar uma URL ou aplicação que não está na base de dados.
4.1.17.4.9 Deve ser possível limitar o consumo de banda de aplicações.
4.1.17.4.10 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;
4.1.17.4.11 Deve ser possível realizar a recategorização de uma URL através da gerência do equipamento.
4.1.17.4.12 Deve ser possível customizar e definir a frequência com que serão exibidas as mensagens para os usuários nas seguintes ações:
4.1.17.4.12.1 Aceitar e informar
4.1.17.4.12.2 Bloquear e informar
4.1.17.4.12.3 Perguntar

4.1.17.5 **Acesso Remoto**
4.1.17.5.1 A solução deve prover acesso seguro encriptado aos usuários remotos através da Internet;
4.1.17.5.2 A solução deve prover conectividade através de um cliente instalado no computador do usuário e através do navegador do usuário com conexão segura (HTTPS).
4.1.17.5.3 Deve suportar pelo menos os seguintes métodos de conexão:
4.1.17.5.3.1 Conexão através de cliente instalado no laptop ou desktop do usuário.
4.1.17.5.3.2 Conexão através de cliente instalado no smartphone e tablets.
4.1.17.5.3.3 Conexão através de navegador com SSL.
4.1.17.5.3.4 Conexão através de cliente nativo Windows L2TP.
4.1.17.5.4 Solução deve suportar alterar a porta padrão 443 para estabelecimento de VPN SSL.
4.1.17.5.5 A solução deve permitir conexão VPN aos seguintes usuários:
4.1.17.5.5.1 Usuários locais na própria base do appliance.
4.1.17.5.5.2 Grupos de usuários locais na própria base do appliance.
4.1.17.5.5.3 Grupos de usuários do Active Directory.
4.1.17.5.5.4 Grupos de usuários Radius.
4.1.17.5.6 A solução deve permitir atribuir um endereço específico para o usuário remoto.

4.1.17.6 **Funcionalidade de VPN Site-to-Site**
4.1.17.6.1 A solução deve prover acesso seguro criptografado entre duas localidades através da Internet;
4.1.17.6.2 A solução deve estabelecer VPN com o site remoto do próprio fabricante ou de terceiros;
4.1.17.6.3 A solução deve suportar autenticação com senha ou certificado;
4.1.17.6.4 Deve suportar, pelo menos, criptografia AES 128 e 256;
4.1.17.6.5 Deve possuir mecanismo para monitorar a saúde do túnel remoto;
4.1.17.6.6 Quando o túnel for estabelecido entre dispositivos do mesmo fabricante este deve possuir protocolo proprietário para testar se o túnel está ativo.

Item 13 - Firewall – UNIDADE REMOTA TIPO III

4.1.17.7 **Características Gerais**
4.1.17.7.1 Throughput de pelo menos 545 Mbps, com as funcionalidades de firewall, prevenção de intrusão e controle de aplicação habilitados simultaneamente;

4.1.17.7.1.1 O Throughput é considerado como a quantidade de tráfego que um único equipamento consegue redirecionar. Não há soma entre o tráfego de entrada e de saída das interfaces;

4.1.17.7.2 Suportar pelo menos 495.000 (quatrocentas e noventa e cinco mil) conexões ou sessões simultâneas;

4.1.17.7.3 Suportar pelo menos 39.000 (trinta e nove mil) novas conexões ou sessões por segundo;

4.1.17.7.4 Throughput de pelo menos 990 Mbps para VPN;

4.1.17.7.5 Possuir pelo menos 16 interfaces de rede 1G UTP;

4.1.17.8 **Funcionalidades Genéricas de Firewall**

4.1.17.8.1 Deve suportar autenticação para o serviço NTP.

4.1.17.8.2 Deve ser possível definir por quais origens são permitidas as conexões do administrador. Por exemplo: LAN, Rede Wireless Confiável, VPN, Internet etc.

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

4.1.17.8.4 Deve suportar SNMP v2 e v3.

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

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

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

4.1.17.8.8 Deve ser possível conectar a serviços de DDNS;

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

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

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

4.1.17.8.12 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;

4.1.17.8.13 A solução deve identificar usuários das seguintes fontes pelo menos:

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

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

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

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

4.1.17.9 **Funcionalidade de Prevenção de Ameaças**

4.1.17.9.1 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.

4.1.17.9.2 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;

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

4.1.17.9.4 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;

4.1.17.9.5 Deve ser capaz de bloquear tráfego SSH em DNS tunneling;

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

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

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

4.1.17.9.9 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;

4.1.17.9.10 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;

4.1.17.9.11 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.

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

4.1.17.9.13 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).

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

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

4.1.17.9.16 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;

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

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

4.1.17.9.19 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.

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

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

4.1.17.9.21.1 Inspecionar tipos de arquivos conhecidos que contenham malware;

4.1.17.9.21.2 Inspecionar todos os tipos de arquivos;

4.1.17.9.21.3 Inspecionar tipos de arquivos de famílias específicas;

4.1.17.9.21.4 Deve bloquear acesso a URLs com malware;

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

4.1.17.10 **Filtro de Conteúdo Web**

4.1.17.10.1 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;

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

4.1.17.10.3 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.

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

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

4.1.17.10.5.1 Usuário do Active Directory

4.1.17.10.5.2 IP
4.1.17.10.5.3 Rede
4.1.17.10.6 Deve ser possível configurar o bloqueio de compartilhamento de arquivos com origem usualmente ilegais como aplicações torrents e peer-to-peer.
4.1.17.10.7 Deve ser possível configurar manualmente o bloqueio de aplicações ou categorias de sites de aplicações indesejadas.
4.1.17.10.8 Deve ainda ser possível adicionar uma URL ou aplicação que não está na base de dados.
4.1.17.10.9 Deve ser possível limitar o consumo de banda de aplicações.
4.1.17.10.10 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;
4.1.17.10.11 Deve ser possível realizar a recategorização de uma URL através da gerência do equipamento.
4.1.17.10.12 Deve ser possível customizar e definir a frequência com que serão exibidas as mensagens para os usuários nas seguintes ações:
4.1.17.10.12.1 Aceitar e informar
4.1.17.10.12.2 Bloquear e informar
4.1.17.10.12.3 Perguntar

4.1.17.11 Acesso Remoto
4.1.17.11.1 A solução deve prover acesso seguro encriptado aos usuários remotos através da Internet;
4.1.17.11.2 A solução deve prover conectividade através de um cliente instalado no computador do usuário e através do navegador do usuário com conexão segura (HTTPS).
4.1.17.11.3 Deve suportar pelo menos os seguintes métodos de conexão:
4.1.17.11.3.1 Conexão através de cliente instalado no laptop ou desktop do usuário.
4.1.17.11.3.2 Conexão através de cliente instalado no smartphone e tablets.
4.1.17.11.3.3 Conexão através de navegador com SSL.
4.1.17.11.3.4 Conexão através de cliente nativo Windows L2TP.
4.1.17.11.4 Solução deve suportar alterar a porta padrão 443 para estabelecimento de VPN SSL.
4.1.17.11.5 A solução deve permitir conexão VPN aos seguintes usuários:
4.1.17.11.5.1 Usuários locais na própria base do appliance.
4.1.17.11.5.2 Grupos de usuários locais na própria base do appliance.
4.1.17.11.5.3 Grupos de usuários do Active Directory.
4.1.17.11.5.4 Grupos de usuários Radius.
4.1.17.11.6 A solução deve permitir atribuir um endereço específico para o usuário remoto.

4.1.17.12 **Funcionalidade de VPN Site-to-Site**

4.1.17.12.1 A solução deve prover acesso seguro criptografado entre duas localidades através da Internet;
4.1.17.12.2 A solução deve estabelecer VPN com o site remoto do próprio fabricante ou de terceiros;
4.1.17.12.3 A solução deve suportar autenticação com senha ou certificado;
4.1.17.12.4 Deve suportar, pelo menos, criptografia AES 128 e 256;
4.1.17.12.5 Deve possuir mecanismo para monitorar a saúde do túnel remoto;
4.1.17.12.6 Quando o túnel for estabelecido entre dispositivos do mesmo fabricante este deve possuir protocolo proprietário para testar se o túnel está ativo.

4.1.18 **Item 14** - Instalação e Configuração de Firewall até 100 KM de Fortaleza
4.1.18.1 Instalação e Configuração de Firewall dos itens 11 a 13 em localidade até 100km distante de Fortaleza

4.1.19 **Item 15** - Instalação e Configuração de Firewall até 400 KM de Fortaleza

4.1.19.1 Instalação e Configuração de Firewall dos itens 11 a 13 em localidade de 100 km até 400 km distante de Fortaleza

4.1.20 **Item 16** - Instalação e Configuração de Firewall acima 400 KM de Fortaleza
4.1.20.1 Instalação e Configuração de Firewall dos itens 11 a 13 em localidade mais de 400 km distante de Fortaleza

4.1.21 **Item 17** - Firewall – CENTRAL TIPO I – AQUISIÇÃO
4.1.21.1 Firewall com as mesmas caracteriticas técnicas do Item 1 (descrito em 4.1.6) deste TR.

4.1.22 **Item 18** - Firewall – CENTRAL TIPO II – AQUISIÇÃO
4.1.22.1 Firewall com as mesmas caracteriticas técnicas do Item 2 (descrito em 4.1.7) deste TR.

4.1.23 **Item 19** - Firewall – CENTRAL TIPO III – AQUISIÇÃO
4.1.23.1 Firewall com as mesmas caracteriticas técnicas do Item 3 (descrito em 4.1.8) deste TR.

4.1.24 **Item 20** - Firewall – CENTRAL TIPO IV – AQUISIÇÃO
4.1.24.1 Firewall com as mesmas caracteriticas técnicas do Item 4 (descrito em 4.1.9) deste TR.

4.1.25 **Item 21** - Firewall – DATA CENTER TIPO I – AQUISIÇÃO
4.1.25.1 Firewall com as mesmas caracteriticas técnicas do Item 5 (descrito em 4.1.10) deste TR.

4.1.26 **Item 22** - Firewall – DATA CENTER TIPO II - AQUISIÇÃO
4.1.26.1 Firewall com as mesmas caracteriticas técnicas do Item 6 (descrito em 4.1.11) deste TR.

4.1.27 **Item 23** - Firewall – DATA CENTER TIPO III – AQUISIÇÃO
4.1.27.1 Firewall com as mesmas caracteriticas técnicas do Item 7 (descrito em 4.1.12) deste TR.

4.1.28 **Item 24** – Gerência Centralizada e Relatoria – TIPO I – AQUISIÇÃO
4.1.28.1 Gerência centralizada e relatoria para até 50 equipamentos, compatível com os firewalls dos itens 11 à 13 deste TR.
4.1.28.2 A solução de gerência centralizada e relatoria ofertada deve atender aos requisitos técnicos descritos no ANEXO A deste TR.

4.1.29 **Item 25** – Gerência Centralizada e Relatoria – TIPO II – AQUISIÇÃO
4.1.29.1 Gerência centralizada e relatoria para ilimitados equipamentos, compatível com os firewalls dos itens 11 à 13 deste TR.
4.1.29.2 A solução de gerência centralizada e relatoria ofertada deve atender aos requisitos técnicos descritos no ANEXO A deste TR.

4.2 DAS CONDIÇÕES DE IMPLANTAÇÃO, GARANTIA, SUPORTE E ASSISTÊNCIA TÉCNICA

4.2.1 Os itens de SERVIÇO, itens 1 a 10, deste TR incluem a implantação, garantia, suporte e assistência técnica conforme descrito abaixo.
4.2.2 É/será de inteira responsabilidade da CONTRATADA a correta instalação, configuração e funcionamento dos equipamentos e componentes da solução ofertada. 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.
4.2.3 Em processos de implantação de mais de 10 ativos deverão ser realizadas as seguintes atividades:
4.2.3.1 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;

4.2.3.2 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.;

4.2.3.3 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;

4.2.3.4 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;

4.2.3.5 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;

4.2.3.6 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;

4.2.4 Em processos de implantação de até 10 ativos os processos detalhados em 4.2.3 podem ser executados de maneira simplificada sendo, no entanto, obrigatório:

4.2.4.1 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;

4.2.4.2 Relatório as-built simplificado;

4.2.4.3 Documentação completa da solução, incluindo especificação do equipamento, características e funcionalidades implementadas, comentários e configurações executadas.

4.2.5 A CONTRATADA deverá possuir uma solução de gerenciamento centralizado e relatórios conforme Anexo A.

4.2.5.1 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.

4.2.6 Todos os equipamentos ou componentes necessários à prestação dos serviços deverão ser novos e de primeiro uso e não constar, no momento da apresentação da proposta, em listas de end-of-sale, end-of-support ou end-of-life do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante.

4.2.7 A Licitante Vencedora deverá apresentar juntamente a sua Proposta uma Carta de cada Fabricante do item proposto declarando que seja Revenda Autorizada/ Parceiro uma empresa capacitada como Prestador de Serviços do Fabricante.

4.2.8 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.

4.2.9 A garantia e cobertura dos serviços será de mesmo prazo do contrato em meses e em caso de necessidade de reparo ou substituição de equipamentos e componentes de algum item fornecido nesse contrato, o mesmo será de responsabilidade da CONTRATADA, devendo ela ainda atender aos critérios/características do equipamento substituído, por outro equivalente ou mesmo superior. O equipamento ou componente que vier a substituir um outro defeituoso, estará sob as mesmas condições de garantia e assistência técnica especificada do que for substituído.

4.2.10 A CONTRATADA substituirá qualquer solução em que o hardware seja avariado por acidentes, operação indevida ou negligente, transporte, intempéries climáticas, vandalismo, descargas elétricas provenientes de raios e trovões, furações, ventanias, inundações, desabamentos e outros desastres naturais dentro de um percentual estipulado de até 5% dos ativos instalados pela CONTRATADA; acima deste percentual a CONTRATANTE se responsabilizará pela aquisição do PCI dentro da vigência do contrato.

4.2.10.1 O percentual de 5% é calculado por item de um contrato que tenha sido efetivamente instalado (emitida uma OS).

4.2.10.2 O CONTRATANTE deixará de fazer os pagamentos daqueles itens que estiverem dentro do percentual de 5% até que este item seja substituído pela CONTRATATADA.

4.2.10.3 O CONTRATANTE continuará fazendo os pagamentos daqueles itens que superar o percentual de 5% que tenha sido avariado independente se o item tenha sido adquirido ou não.

4.2.11 Para garantir a qualidade e disponibilidade do serviço, deverá ser disponibilizado pela empresa CONTRATADA uma ferramenta de gerência e visibilidade 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.

4.2.11.1 Fica a critério da ETICE a solicitação desta ferramenta a qualquer momento após a contratação de pelo menos 20 ativos usando esse Termo de Referência

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

4.2.11.3 A ferramenta pode ser fornecido em forma de appliance ou máquina virtual;

4.2.11.3.1 Caso seja ofertado appliance virtual, este deve ser compatível e homologado para operação com VMware;

4.2.11.3.2 Caso seja ofertado appliance físico, o equipamento deve possuir:

4.2.11.3.2.1 Pelo menos 2 interfaces 1000Base-T com conectores RJ-45;

4.2.11.3.2.2 Porta console padrão RJ-45, USB ou RS-232 para permitir o gerenciamento completo através de linha de comando;

4.2.11.3.2.3 Possuir indicadores luminosos (led) para a indicação do status;

4.2.11.3.2.4 Fonte de alimentação com capacidade para operar em tensões de 110V / 220V com comutação automática. Deve acompanhar fonte de alimentação redundante interna com operação N+1;

4.2.12 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.

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

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

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

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

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

4.2.13.5 Suporte em criação de políticas, configurações, parametrizações de quaisquer ordem relativos aos equipamentos ofertados;

4.2.13.6 Resolução de problemas referente a políticas, configurações, parametrizações de quaisquer ordem relativos aos equipamentos ofertados;

4.2.13.7 Suporte a criação, geração e parametrização de relatórios e eventos de segurança de quaisquer natureza detectados e prevenidos pelos equipamentos ofertados;

4.2.13.8 Encaminhar incidentes ao fabricante da solução;

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

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

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

4.2.14 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.

4.2.15 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.

4.2.16 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.

4.2.17 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.

4.2.18 . 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.

4.2.19 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:

4.2.19.1 02 (dois) profissionais com nível professional na solução ofertada

4.2.19.2 02 (dois) profissionais com nível expert na solução ofertada;

4.2.19.3 02 (dois) profissionais com certificação ITIL Foudation;

4.2.19.4 01 (um) profissional com certificação PMP;

4.2.20 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.

4.2.21 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).

4.2.22 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 ór-

gão/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).

4.2.23 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.

4.2.24 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 da mesma, mesmo que a falha não tenha sido consumada, mas que tenha sido detectada a existência do risco.

4.2.25 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.

4.2.26 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:

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

4.2.26.2 Operação impactada (incidente que gere parada parcial de algum serviço contemplado nesse contrato) o tempo de atendimento será de até 4 (quatro) horas.

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

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

4.2.27 Quando do encerramento da prestação de serviços formada em Contrato, a CONTRATADA deverá retirar todos os equipamento e componentes alocados na solução, e, para tanto comunicando a data de retirada à CONTRATANTE, por escrito, 30 (trinta) dias de antecedência.

4.3. DAS CONDIÇÕES DE GARANTIA, SUPORTE E ASSISTÊNCIA TÉCNICA PARA OS ITENS DE AQUISIÇÃO

4.3.1. Os itens de AQUISIÇÃO, itens 11 a 13 e 17 a 25, deste TR devem oferecer as condições de garantia conforme descrito abaixo.

4.3.2. A garantia deverá ser integral de, no mínimo, **36 (trinta e seis) meses do fabricante**, com cobertura total para peças e serviços.

4.3.3. 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;

4.3.5. 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 outras 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 CONTRATANTE, a ser informada quando da lavratura do instrumento contratual.

6. DA EXECUÇÃO E DO RECEBIMENTO

6.1. **Quanto à execução:**

6.1.1. O objeto contratual deverá ser executado em conformidade com as especificações estabelecidas neste instrumento, em um prazo máximo de 90 (noventa) dias úteis contado a partir do recebimento da ordem de serviço ou instrumento hábil.

6.1.2. 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) órgão(s)/entidade(s) participante(s) do SRP (Sistema de Registro de Preços) 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.

7.1.1. 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.

7.2. Não será efetuado qualquer pagamento à CONTRATADA, em caso de descumprimento das condições de habilitação e qualificação exigidas na licitação.

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

7.4. 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.

7.4.1. 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.

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

7.5.1. 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.

7.6. 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:

8.1.1. Pela inexecução total ou parcial do contrato, a contratante poderá, garantida a prévia defesa, aplicar a contratada, nos termos do art. 83 da Lei nº 13.303/2016, as seguintes penalidades:

8.1.1.1. Advertência

8.1.1.2. Multas, estipuladas na forma a seguir:

a) Multa de 0,2% (dois décimos por cento) do valor do contrato por dia de atraso, até o máximo de 5% (cinco 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 e rescisão contratual, exceto se houver justificado interesse público em manter a avença, hipótese em que será aplicada apenas a multa.

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. A aplicação da presente multa exclui a aplicação da multa prevista na alínea anterior.

d) Multa 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.

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.

8.2. 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.

8.2.1. 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.

8.2.2. A multa poderá ser aplicada com outras sanções segundo a natureza e a gravidade da falta cometida, desde que observado o princípio da proporcionalidade e o previsto no art. 166 e seguintes – Das Sanções Administrativas do Regulamento Interno de Licitações e Contratos da ETICE.

8.3. Dos demais órgãos da administração pública

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

8.3.1.1. Multas, estipuladas na forma a seguir:

a) Multa de 0,2% (dois décimos por cento) do valor do contrato por dia de atraso, até o máximo de 5% (cinco 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. 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.

8.3.1.2. 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.

8.4. 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.

8.4.1. 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.

8.5. 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. 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.

9.4. 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.

9.5. 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.

9.6. 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.

9.7. 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.

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

9.9. 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.

9.10. 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.

9.10.1. 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.

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 gestor especialmente designado para este fim pela contratante, a ser informado quando da lavratura do instrumento contratual.

12. PRAZO DE VIGÊNCIA DA ATA DE REGISTRO DE PREÇOS

12.1. A Ata de Registro de Preços terá validade pelo prazo de 12 (doze) meses, contados a partir da data da sua publicação.

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 para os itens 1 a 10 serão de 36 (trinta e seis) meses, 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 para os itens 11 a 25 serão de 12 (doze) meses, a partir da celebração do contrato conforme disposto no art. 71 da Lei nº 13.303/2016.

14.3. Os prazos de vigência e de execução poderão ser prorrogados nos termos do que dispõe o art. 71 e 81 da Lei Federal nº 13.303/2016.

14.4. A publicação resumida deste contrato dar-se-á nos termos do § 2º do art. 51 da Lei nº 13.303/2016.

15. DOS ANEXOS DO TERMO DE REFERÊNCIA

ANEXO A - GERENCIAMENTO CENTRALIZADO E RELATÓRIOS

ANEXO B - CARACTERÍSTICAS DA SOLUÇÃO DE MONITORAMENTO

ANEXO C - ÓRGÃOS PARTICIPANTES

Responsável pela elaboração do Termo de Referência:

_____

Álvaro Claudio Maia

Diretor de Tecnologia e Inovação - ETICE

ANEXO A
GERENCIAMENTO CENTRALIZADO E RELATÓRIOS

1. Caso a solução possua licenças relacionadas a armazenamento, deve ser ofertada uma licença de capacidade ilimitada;
2. Deve possuir solução de gerenciamento e administração centralizado, possibilitando o gerenciamento de diversos equipamentos de proteção de rede desde que não sejam software livre;
3. Os equipamentos dos tipos 1 a 7 devem ser gerenciados e administrados através deste módulo;
4. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança;
5. Centralizar a administração de regras e políticas dos equipamentos de proteção de rede dos itens 1 a 7, usando uma única interface de gerenciamento;
6. O gerenciamento da solução deve suportar acesso via SSH, cliente e WEB (HTTPS);
7. O gerenciamento deve permitir/possuir monitoração de logs, ferramentas de investigação de logs e acesso concorrente de administradores;
8. Suportar criação de regras que fiquem ativas em horário definido;
9. Suportar criação de regras com data de expiração;
10. Suportar backup das configurações e rollback de configuração para a última configuração salva;
11. Suportar validação de regras antes da aplicação;
12. Suportar validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);
13. Deve possibilitar a integração com outras soluções de SIEM de mercado desde que não sejam software livre;
14. Suportar geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;
15. Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e Anti-Malware), etc;
16. Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus, Anti-Malware), e URLs que passaram pela solução;
17. Deve ser possível exportar os logs em CSV;
18. Deve possibilitar a geração de relatórios no formato PDF;
19. Possibilitar rotação do log;
20. Suportar geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:

1.20.1. 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;

21. Deve permitir a criação de relatórios personalizados;
22. Suportar enviar os relatórios de forma automática via e-mail em PDF ou HTML;
23. Deve consolidar logs e relatórios de todos os dispositivos administrados;
24. Capacidade de definir administradores com diferentes perfis de acesso com, no mínimo, as permissões de Leitura/Escrita e somente Leitura;
25. Deverá possuir mecanismo de Drill-Down para navegação e análise dos logs em tempo real;
26. Nas opções de Drill-Down, deve ser possível identificar o usuário que fez determinado acesso;
27. Suportar gerar relatórios de aderência às políticas de negócio;
28. Suportar gerar alertas não aderentes às políticas de negócio;

29. A solução de gerenciamento deverá ser entregue como appliance virtual e deve ser compatível/homologado para VMware ESXi versão 5 e superior
30. Permitir a integração e avaliação de todos os equipamentos de proteção de rede dos tipos 1 a 11 na gerência com os seguintes padrões regulatórios:

30.1 ISO 27002;

30.2 GDPR

31 Simular o impacto de segurança das alterações de configuração antes da instalação de acordo com a aderência aos padrões regulatórios apresentados no item anterior;

32 Permtir a customização do padrão regulatório da própria instituição;

33 Pemitir notificação instantânea sobre mudanças de política de segurança que impactam negativamente a segurança;

34 Monitar constantemente o status de conformidade da solução aos padrões regulatórios informados;

35 Possuir status de segurança com atualização automática a cada alteração de configuração;

36 Possuir alertas de políticas e as potenciais violações de conformidade;

37 Gerar relatórios regulamentares com base nas configurações de segurança em tempo real;

38 Permitir que os relatórios possam ser salvos, enviados e impressos;

39 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 e gerenciamento das funcionalidades adquiridas de todos os equipamentos e softwares ofertados;

40 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;

41 A solução deve prover, no mínimo, as seguintes funcionalidades para análise avançada dos incidentes:

41.1 Visualizar quantidade de tráfego utilizado de aplicações e navegação;

41.2 Gráficos com principais eventos de segurança de acordo com a funcionalidade selecionada;

42 A solução deve ser capaz de detectar ataques de tentativa de login e senha;

43 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;

44 A solução deve permitir gerenciar mudanças com segurança automatizada;

45 A solução deve permitir o controle de alterações de forma visual e através de relatórios;

46 A solução deve possuir processo automático, formal para o acompanhamento, aprovação e alterações de política de segurança;

47 A solução deve suportar notificação por e-mail acerca das instalações de políticas;

48 Deve permitir a customização de dashboards da solução de gerenciamento;

49 A solução deverá prover funcionalidade para apoiar nos processos internos de gerência de mudanças e gerência de configuração;

50 A solução deve possibilitar o funcionamento em modo de auditoria provendo a possibilidade de auditar todas as mudanças de políticas com relatório detalhado de cada alteração efetuada;

51 A solução deve permitir um fluxo de aprovação da alteração efetuada para possibilitar que somente alterações gerencialmente aprovadas poderão ser efetivamente aplicadas;

52 A solução deverá prover um relatório detalhado da alteração para que seja possível uma revisão da alteração antes da aprovação;

53 Permitir criações de políticas de acesso de usuários autenticados no Active Directory, de forma que reconheça os usuários de forma transparente;

54 Permitir o download de assinaturas, atualizações e firmwares para distribuição centralizada aos dispositivos de segurança integrados a mesma;

55 Permitir a visualização de gráficos e mapa de ameaças;
56 Possuir mecanismo para que logs antigos sejam removidos automaticamente;
57 Possuir a capacidade de personalização de gráficos;
58 Deve permitir a criação de dashboards customizados para visibilidades do tráfego de aplicativos, categorias de URL, ameaças, serviços, países, origem e destino;
59 Deve possuir a capacidade de visualizar na interface gráfica da solução de relatórios informações do sistema como licenças, memória, disco, uso de CPU, taxa de logs por segundo recebidos, total de logs diários recebidos, alertas gerados entre outros;
60 Deve ser capaz de personalizar e criar regras de correlação;
61 Deve fornecer uma interface gráfica para criação das regras citadas no item anterior;
62 Deve possuir painéis de eventos em tempo real com possibilidade de configuração das atualizações e frequências;
63 Deve disponibilizar a geração de pelo menos os seguintes tipos de relatórios:
64 Máquinas mais acessadas, serviços mais utilizados, usuários que mais utilizaram serviços, URLs mais visualizadas e categorias Web mais acessadas;
65 Deve permitir a integração com sistemas terceiros através de API;
66 Deve permitir a criação de objetos e políticas compartilhadas;
67 Deve suportar configuração em alta disponibilidade para fins de redundância;

ANEXO B

CARACTERÍSTICAS DA SOLUÇÃO 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 compatíveis 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;
   6.11. 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;
   8.1. Deve suportar o monitoramento através do protocolo SNMP nas versões 1, 2c e 3 e SNMP Traps;
9. Análise, relatórios e comparação:
   9.1. Armazenar informações para posterior análise, que possa permitir comparações para acertos nos equipamentos.
   9.2. A solução deverá possuir uma interface interna para geração de relatórios.

9.3. A solução deve possuir interface WEB para geração e visualização de relatórios.
9.3.1. 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.
9.4. A solução deve possibilitar a exportação dos relatórios em pelo menos dois dos seguintes formatos:
9.4.1. PDF.
9.4.2. HTML.
9.4.3. CSV.
9.5. Todos os relatórios devem ter a flexibilidade de exibir informações em tempo real e também dados históricos, coletados em períodos anteriores.
9.6. 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:
9.6.1. Apresentação dos nomes dos equipamentos no relatório.
9.6.2. Apresentação das informações gerenciadas por equipamento.
9.6.3. Exibição por grupo de equipamentos previamente estabelecidos.
9.7. Opções de periodicidade especificada pelo usuário: diária, semanal, mensal, trimestral, anual ou intervalo de data.
10. Apresentação em modo gráfico:
10.1. A solução deverá permitir a criação de gráficos unitários ou em conjunto de qualquer item de Monitoramento, permitindo assim, uma análise cruzada entre os vários dados monitorados;
10.2. 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

	Órgão/Entidade
01	**ETICE** - Empresa de Tecnologia da Informação do Ceará - Av. Pontes Vieira, 220 - São João do Tauape. CEP: 60.130-240. Fortaleza-CE.
02	**SEDUC** - Av. General Afonso Albuquerque Lima, s/n - Cambeba Fortaleza, CE - CEP: 60.822-325

ANEXO II - CARTA PROPOSTA

À

Central de Licitações do Estado do Ceará.

Ref.: Pregão Eletrônico nº 20190013 – 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	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 20190013-ETICE

PROCESSO Nº 10314312/2019.

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 20190013 - ETICE do respectivo resultado homologado, publicado no Diário Oficial do Estado em __/__/20__, às fls ____, do Processo nº **10314312/2019**, 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 20190013 – 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 a Lei Federal nº 13.303, de 30.6.2016.

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 com 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 20190013 - 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 **10314312/2019**.

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, a ETICE poderá firmar contratos com os fornecedores com preços registrados.

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.

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 ao órgão participante, 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 os pedidos efetuados 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 pelo participante do Sistema de Registro de Preços.

c) Responder no prazo de até 5 (cinco) dias a consultas do órgão gestor de Registro de Preços sobre a pretensão de órgão/entidade não participante.

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 único deste 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 o órgão participante/interessados e o prestador de serviço.

Subcláusula Primeira – Caso o prestador de serviço classificado em primeiro lugar, não cumpra o prazo estabelecido pelos órgãos participantes, ou se recuse a executar o serviço, terá o seu registro de preço cancelado, sem prejuízo das demais sanções previstas em lei e no instrumento contratual.

Subcláusula Segunda – Neste caso, o órgão participante comunicará ao órgão gestor, competindo a este convocar sucessivamente por ordem de classificação, os demais prestadores de serviços.

CLÁUSULA DÉCIMA PRIMEIRA - DA EXECUÇÃO E DO RECEBIMENTO

Subcláusula Primeira - Quanto à execução

a) O objeto contratual deverá ser executado em conformidade com as especificações estabelecidas neste instrumento, em um prazo máximo de 90 (noventa) dias úteis contado a partir do recebimento da ordem de serviço ou instrumento hábil.

b) 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.

Subcláusula Segunda - Quanto ao recebimento:

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

b) DEFINITIVAMENTE, sendo expedido termo de recebimento definitivo, após verificação da qualidade e da 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 SEGUNDA - DO PAGAMENTO

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.

Subcláusula Primeira - 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.

Subcláusula Segunda - Não será efetuado qualquer pagamento à CONTRATADA, em caso de descumprimento das condições exigidas no processo licitatório.

Subcláusula Terceira - É vedada a realização de pagamento antes da execução do objeto ou se o mesmo não estiver de acordo com as especificações do Anexo I - Termo de Referência do edital do Pregão Eletrônico nº 20190013 - ETICE.

Subcláusula Quarta - 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.

Subcláusula Quinta - 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.

Subcláusula Sexta - Os pagamentos encontram-se ainda condicionados à apresentação dos seguintes comprovantes:

a) 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.

Subcláusula Sétima - 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 DÉCIMA TERCEIRA - DAS SANÇÕES ADMINISTRATIVAS

Subcláusula Primeira – O prestador de serviço que praticar quaisquer das condutas previstas no art. 32, do Decreto Estadual nº 28.089/2006, 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), podendo ser substituído por outro instrumento legal, em nome do órgão contratante. Se não o fizer, será cobrada em processo de execução.

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

CLÁUSULA DÉCIMA QUARTA - DA FRAUDE E DA CORRUPÇÃO

O detentor de preços registrado 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.

Subcláusula Primeira - 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.

Subcláusula Segunda- 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.

Subcláusula Terceira - 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 QUINTA - DO FORO

Fica eleito o foro do município de Fortaleza, capital 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 20190013 - ETICE.

Item	Cód Item	Especificação do Item	Fornecedores Por Ordem de Classificação	Qtde	Unidade	Preço Registrado do Item(R$)	Valor Total (R$)

ANEXO IV - MINUTA DO CONTRATO

CONTRATO Nº ____ / _____.

PROCESSO Nº 10314312/2019 - 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° 20190013 - ETICE e seus anexos, os preceitos do direito público, e a Lei Federal nº 8.666/1993, o Regulamento de Interno de Licitações e Contratos da ETICE e, ainda, 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 20190013 - 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 as contratações de solução de proteção de redes incluindo aquisições de hardware e software e respectivo serviço de implantação, posterior monitoramento e com 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 20190013 - 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 - DO VALOR E DO REAJUSTAMENTO DO PREÇO

5.1. O valor 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.

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.

6.1.1. 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.

6.2. Não será efetuado qualquer pagamento à CONTRATADA, em caso de descumprimento das condições exigidas no processo licitatório.

6.3. É vedada a realização de pagamento antes da execução do objeto ou se o mesmo não estiver de acordo com as especificações do Anexo I - Termo de Referência do edital do Pregão Eletrônico n° 20190013 - ETICE.

6.4. 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.

6.4.1. 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.

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

6.5.1. 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.

6.6. 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 para os itens 1 a 10 serão de 36 (trinta e seis) meses, a partir a partir do recebimento da ordem de serviço ou ordem de fornecimento.

8.2. Os prazos de vigência e de execução contratual para os itens 11 a 25 serão de 12 (doze) meses, a partir do recebimento da ordem de serviço ou ordem de fornecimento.

8.3. Os prazos de vigência e de execução poderão ser prorrogados nos termos do art. 57 da Lei Federal n° 8.666/1993.

CLÁUSULA NONA - DA GARANTIA CONTRATUAL

9.1. 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 13.303/2016. Na ocorrência de acréscimo contratual de valor, deverá ser prestada garantia proporcional ao valor acrescido, nas mesmas condições inicialmente estabelecidas.

CLÁUSULA DÉCIMA - DA EXECUÇÃO E DO RECEBIMENTO

10.1. Quanto à execução:

10.1.1. O objeto contratual deverá ser executado em conformidade com as especificações e locais indicados no Anexo C do Termo de Referência do Edital.

10.1.2. Os atrasos ocasionados por motivo de força maior ou caso fortuito, desde que justificados até 02 (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. 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.

11.4. 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.

11.5. 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.

11.6. 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.

11.7. 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 n.º 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. 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.

11.10.1. 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 pelo (a) _____, especialmente designado (a) para este fim pela CONTRATANTE, de acordo com o estabelecido no art. 67, da Lei Federal nº 8.666/1993, doravante denominada simplesmente de GESTOR (A).

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 0,2% (dois décimos por cento) do valor do contrato por dia de atraso, até o máximo de 5% (cinco 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. 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.

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 do órgão CONTRATANTE. Se não o fizer, será cobrado em processo de execução.

14.3. 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, e que não constitua o escopo principal do objeto, restrita, contudo, ao percentual máximo de 30% (trinta por cento) da contratação.

16.2. A subcontratação de que trata esta cláusula, não exclui a responsabilidade da contratada perante a contratante quanto à qualidade técnica da obra ou do serviço prestado, não constituindo portanto qualquer vínculo contratual ou legal da contratante com a subcontratada.

16.3. A contratada ao requerer autorização para subcontratação de parte do objeto, deverá comprovar perante a Administração a regularidade jurídico/fiscal e trabalhista de sua subcontratada.

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.

17.2. Este contrato poderá ser rescindido a qualquer tempo pela CONTRATANTE, mediante aviso prévio de no 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 V - MINUTA DO CONTRATO - ESTATAIS

Contrato nº ____ / _____

Processo nº 10314312/2019-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° 20190013 e seus Anexos, os preceitos do direito público, e a Lei Federal nº 13.303/2016, com suas alterações, e, ainda, 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 20190013 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 com 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 20190013 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 valor 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.

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.

6.1.1. 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.

6.2. Não será efetuado qualquer pagamento à CONTRATADA, em caso de descumprimento das condições exigidas no processo licitatório.

6.3. É vedada a realização de pagamento antes da execução do objeto ou se o mesmo não estiver de acordo com as especificações do Anexo I – Termo de Referência do edital do Pregão Eletrônico n° 20190013.

6.4. 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.

6.4.1. 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.

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

6.5.1. 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.

6.6. 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 para os itens 1 a 10 serão de 36 (trinta e seis) meses, a partir da celebração do contrato conforme disposto no art. 71 da Lei nº 13.303/2016.

8.2. Os prazos de vigência e de execução contratual para os itens 11 a 25 serão de 12 (doze) meses, a partir da celebração do contrato conforme disposto no art. 71 da Lei nº 13.303/2016.

8.3 Os prazos de vigência e de execução poderão ser prorrogados nos termos do que dispõe o art. 57, § 1o da Lei Federal n° 8.666/1993, e no caso no caso das empresas públicas, economia mista e suas subsidiárias, de acordo com o art. 71 da Lei Federal nº 13.303/2016,

8.4. A publicação resumida deste contrato dar-se-á na forma do parágrafo único, do art. 61, da Lei Federal nº 8.666/1993 e para as empresa públicas, economia mista e suas subsidiárias, nos termos do § 2º do art. 51 da Lei nº 13.303/2016.

CLÁUSULA NONA – DA GARANTIA CONTRATUAL

9.1. 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 13.303/2016. Na ocorrência de acréscimo contratual de valor, deverá ser prestada garantia proporcional ao valor acrescido, nas mesmas condições inicialmente estabelecidas.

CLÁUSULA DÉCIMA – DA EXECUÇÃO E DO RECEBIMENTO

10.1. Quanto à execução:

10.1.1. OO objeto contratual deverá ser executado em conformidade com as especificações e locais indicados no anexo B do Termo de Referência do Edital.

10.1.2. 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. 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.

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.

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 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, observando o prazo mínimo exigido pela Administração.

11.9. Providenciar a substituição de qualquer profissional envolvido na execução do objeto contratual, 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 n.º 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. 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 frequencia dos presos e egressos e/ou jovens do sistema socieducativo, 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 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 contrato.

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 pelo (a) _____, especialmente designado (a) para este fim pela CONTRATANTE, doravante denominada simplesmente de GESTOR (A).

CLÁUSULA DÉCIMA QUARTA – DAS SANÇÕES ADMINISTRATIVAS

14.1. Pela inexecução total ou parcial do contrato, a contratante poderá, garantida a prévia defesa, aplicar a contratada, nos termos do art. 83 da Lei nº 13.303/2016, as seguintes penalidades:

14.1.1. Advertência

14.1.2. Multas, estipuladas na forma a seguir:

a) Multa de 0,2% (dois décimos por cento) do valor do contrato por dia de atraso, até o máximo de 5% (cinco 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 e rescisão contratual, exceto se houver justificado interesse público em manter a avença, hipótese em que será aplicada apenas a multa.

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. A aplicação da presente multa exclui a aplicação da multa prevista na alínea anterior;

d) Multa 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.

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. 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.

14.2.1. 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.

14.2.2. A multa poderá ser aplicada com outras sanções segundo a natureza e a gravidade da falta cometida, desde que observado o princípio da proporcionalidade e o previsto no art. 166 e seguintes – Das Sanções Administrativas do Regulamento Interno de Licitações e Contratos da ETICE.

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, e que não constitua o escopo principal do objeto, restrita, contudo, ao percentual máximo de 30% (trinta por cento) da contratação.

16.2. A subcontratação de que trata esta cláusula, não exclui a responsabilidade da contratada perante a contratante quanto à qualidade técnica da obra ou do serviço prestado, não constituindo portanto qualquer vínculo contratual ou legal da contratante com a subcontratada.

16.3. A contratada ao requerer autorização para subcontratação de parte do objeto, deverá comprovar perante a Administração a regularidade jurídico/fiscal e trabalhista de sua subcontratada.

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.

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)
CONTRATANTE

(nome do representante)
CONTRATADO(A)

Testemunhas:

(nome da testemunha 1)
RG:
CPF:

(nome da testemunha 2)
RG:
CPF:

Visto:

(Nome do(a) procurador(a)/assessor(a) jurídico(a) da CONTRATANTE)

ANEXO 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)