

PREGÃO ELETRÔNICO Nº 047/2020-MP/PA
(Processo Administrativo n.º 162/2019-SGJ-TA)

Torna-se público que o **MINISTÉRIO PÚBLICO DO ESTADO DO PARÁ**, por intermédio do(a) Pregoeiro(a) designado pela **Portaria n.º 3126/2020-MP/PGJ, de 04/11/2020**, sediado na Rua João Diogo nº 100, bairro Cidade Velha, CEP: 66015-165, realizará, por solicitação do **Departamento de Informática (protocolo 45212/2019)**, licitação, **para registro de preços**, na modalidade PREGÃO, na forma ELETRÔNICA, com **critério de julgamento menor preço por grupo, modo de disputa “aberto”**, nos termos da Lei nº 10.520, de 17 de julho de 2002, do Decreto n.º 10.024, de 20 de setembro de 2019, Decreto Estadual 534, de 05 de fevereiro de 2020, Decreto Estadual 991, de 24 de agosto de 2020, do Decreto nº 7.746, de 05 de junho de 2012, do Decreto nº 7.892, de 23 de janeiro e 2013, da Instrução Normativa SLTI/MP nº 01, de 19 de janeiro de 2010, da Instrução Normativa SEGES/MP nº 03, de 26 de abril, de 2018, da Lei Complementar nº 123, de 14 de dezembro de 2006, da Lei nº 11.488, de 15 de junho de 2007, do Decreto nº 8.538, de 06 de outubro de 2015, aplicando-se, subsidiariamente, a Lei nº 8.666, de 21 de junho de 1993, e as exigências estabelecidas neste Edital.

Data da sessão: 09 DE MARÇO DE 2021

Horário: 09:30h (NOVE E TRINTA) HORAS – HORÁRIO DE BRASÍLIA

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

UASG: 925980

1. DO OBJETO

- 1.1. O objeto da presente licitação é a escolha da proposta mais vantajosa para **Registro de Preços para a aquisição de ativos de segurança de rede, Firewalls Next Generation (NGFW) com SD-WAN integrada, contemplando os serviços de Instalação, Treinamento e Suporte Técnico**, conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.
- 1.2. A licitação será realizada em **grupo único, formado por 06 itens**, conforme tabela constante no Termo de Referência, devendo o licitante oferecer proposta para todos os itens que o compõem.
- 1.3. O critério de julgamento adotado será o **menor preço GLOBAL do grupo**, observadas as exigências contidas neste Edital e seus Anexos quanto às especificações do objeto.
- 1.4. **Em caso de divergência entre a descrição e/ou descrição detalhada do item cadastrada no [comprasgovernamentais](http://www.comprasgovernamentais.gov.br) e as consignadas no termo de referência, prevalecem as consignadas no termo de referência.**

2. DOS RECURSOS ORÇAMENTÁRIOS

- 2.1. Os recursos financeiros para atender às despesas decorrentes desta licitação estão previstos na dotação orçamentária, sob a seguinte classificação funcional programática:
Classificação: 12101.03.122.1494.8760 – Governança e Gestão
Elemento: 4490-52 – Equipamentos e Material Permanente
Fonte: 0301 – Recursos Ordinários
Elemento: 3390-40 – Serviços da Tecnologia da Informação e Comunicação
Fonte: 0101 – Recursos Ordinários

3. DO CREDENCIAMENTO

- 3.1. O Credenciamento é o nível básico do registro cadastral no SICAF, que permite a participação dos interessados na modalidade licitatória Pregão, em sua forma eletrônica.
- 3.2. O cadastro no SICAF deverá ser feito no Portal de Compras do Governo Federal, no sítio www.comprasgovernamentais.gov.br, por meio de certificado digital conferido pela Infraestrutura de Chaves Públicas Brasileira – ICP - Brasil.
- 3.3. O credenciamento junto ao provedor do sistema implica a responsabilidade do licitante ou de seu representante legal e a presunção de sua capacidade técnica para realização das transações inerentes a este Pregão.

- 3.4. O licitante responsabiliza-se exclusiva e formalmente pelas transações efetuadas em seu nome, assume como firmes e verdadeiras suas propostas e seus lances, inclusive os atos praticados diretamente ou por seu representante, excluída a responsabilidade do provedor do sistema ou do órgão ou entidade promotora da licitação por eventuais danos decorrentes de uso indevido das credenciais de acesso, ainda que por terceiros.
- 3.5. É de responsabilidade do cadastrado conferir a exatidão dos seus dados cadastrais no SICAF e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados.
 - 3.5.1. A não observância do disposto no subitem anterior poderá ensejar desclassificação no momento da habilitação

4. DA PARTICIPAÇÃO NO PREGÃO.

- 4.1. Poderão participar deste Pregão interessados cujo ramo de atividade seja compatível com o objeto desta licitação, e que estejam com Credenciamento regular no Sistema de Cadastramento Unificado de Fornecedores – SICAF, conforme disposto no art. 9º da IN SEGES/MP nº 3, de 2018.
 - 4.1.1. Os licitantes deverão utilizar o certificado digital para acesso ao Sistema.
 - 4.1.2. Aplica-se neste certame o previsto na Lei Complementar 123/2006, de 14 de dezembro de 2006, que estabelece normas gerais relativas ao tratamento diferenciado e favorecido a ser dispensado às microempresas e empresas de pequeno porte;
 - 4.1.2.1. As microempresas (ME) e empresas de pequeno porte (EPP) que quiserem usufruir dos benefícios concedidos pela LC nº 123/2006 deverão declarar em campo próprio do sistema eletrônico a sua condição de ME ou EPP.
 - 4.1.2.2. A mera declaração como ME ou EPP ou a efetiva utilização dos benefícios concedidos pela LC nº 123/2006 por licitante que não se enquadra na definição legal reservada a essas categorias configura fraude ao certame, sujeitando a mesma à aplicação de penalidade de impedimento de licitar e contratar com a Administração Pública, além de ser descredenciada do SICAF, pelo prazo de até 5 (cinco) anos, sem prejuízo das multas previstas neste Edital e das demais cominações legais.
 - 4.1.2.3. O **Grupo Único** deste certame, cujo valor estimado é superior a R\$80.000,00 (oitenta mil reais), **NÃO** possuirá cota destinada exclusivamente à participação de microempresas e empresas de pequeno porte, pois envolve a contratação de serviços e devido a necessidade alegada de compatibilidade técnica entre os itens, conforme art. 48, III, Lei Complementar 123/2006, de 14 de dezembro de 2006;
 - 4.1.3. Como condição de participação, em conformidade com o ACÓRDÃO TCU nº 1793/2011-Plenário (itens 9.5.1.5, 9.5.1.6 e 9.5.1.8) será verificada ainda:
 - 4.1.3.1. A existência de registros impeditivos da contratação:**
 - I. No módulo Sicaf do sistema Siasg;
 - II. No Cadastro Nacional de Empresas Inidôneas e Suspensas/CGU, disponível no Portal da Transparência (<http://www.portaltransparencia.gov.br>);
 - III. No Cadastro Nacional de Condenações Cíveis por Ato de Improbidade Administrativa disponível no Portal do CNJ;
 - IV. As consultas II e III podem ser substituídas pela Consulta Consolidada de Pessoa Jurídica, no site <https://certidoes-apf.apps.tcu.gov.br>.
 - 4.1.3.2. A composição societária das empresas** a serem contratadas no sistema Sicaf a fim de certificarem se entre os sócios há servidores do próprio órgão/entidade contratante, abstendo-se de celebrar contrato nessas condições, em atenção ao art. 9º, inciso III, da Lei nº 8.666/1993;

- 4.1.3.3. No Portal da Transparência (<http://www.portaldatransparencia.gov.br>), quando da habilitação de microempresa e de empresa de pequeno porte, que tenha utilizado a prerrogativa de efetuar lance de desempate, conforme Lei Complementar nº 123/2006, art. 44, **se o somatório de ordens bancárias recebidas pela empresa**, relativas ao seu último exercício, já seria suficiente para extrapolar o faturamento máximo permitido como condição para esse benefício, conforme art. 3º da mencionada Lei Complementar;
- 4.2. Não poderão participar desta licitação os interessados:
- 4.2.1. Proibidos de participar de licitações e celebrar contratos administrativos, na forma da legislação vigente;
- 4.2.2. Que não atendam às condições deste Edital e seu(s) anexo(s);
- 4.2.3. Estrangeiros que não tenham representação legal no Brasil com poderes expressos para receber citação e responder administrativa ou judicialmente;
- 4.2.4. Que se enquadrem nas vedações previstas no artigo 9º da Lei nº 8.666, de 1993;
- 4.2.5. Que estejam sob falência, concurso de credores, concordata ou em processo de dissolução ou liquidação;
- 4.2.6. Organizações da Sociedade Civil de Interesse Público - OSCIP, atuando nessa condição (Acórdão nº 746/2014-TCU-Plenário).
- 4.2.7. Empresas com sócios administradores ou representantes em comum, se participantes do mesmo item;
- 4.2.8. Empresas controladoras, coligadas ou subsidiárias entre si;
- 4.2.9. As empresas com "**Ocorrência de Impedimento Indireto**" no SICAF, conforme a manifestação do Controle Interno deste Parquet nos protocolos 24777/2017 e 38839/2018.
- 4.2.10. Empresa que tenha entre seus empregados colocados à disposição do Ministério Público para o exercício de funções de chefia, pessoas que incidam na vedação dos arts. 1º e 2º da **Resolução nº 177/2017-CNMP**:
- 4.2.10.1. Pessoa que tenha sido condenada em decisão com trânsito em julgado ou proferida por órgão jurisdicional colegiado, nos seguintes casos:
- I – atos de improbidade administrativa;
- II – crimes:
- a) contra a administração pública;
- b) contra a incolumidade pública;
- c) contra a fé pública;
- d) contra o patrimônio;
- e) de abuso de autoridade, nos casos em que houver condenação à perda do cargo ou à inabilitação para o exercício de função pública;
- f) de tráfico de entorpecentes e drogas afins, racismo, tortura, terrorismo e hediondos;
- g) contra a vida e a dignidade sexual;
- h) praticados por organização ou associação criminosa;
- i) de redução de pessoa à condição análoga à de escravo;
- j) eleitorais, para os quais a lei comine pena privativa de liberdade;
- k) de lavagem ou ocultação de bens, direitos e valores.
- 4.2.10.2. Aqueles que tenham:
- I – praticado atos causadores da perda do cargo ou emprego público, reconhecidos por decisão transitada em julgado ou proferida por órgão judicial colegiado;
- II – sido excluídos do exercício da profissão, por decisão definitiva sancionatória judicial ou administrativa do órgão profissional competente, salvo se o ato houver sido anulado ou suspenso pelo Poder Judiciário;
- III – tido suas contas relativas ao exercício de cargos ou funções públicas rejeitadas por irregularidade insanável que configure ato doloso de improbidade

administrativa, por decisão irrecurável do órgão competente, salvo se esta houver sido suspensa ou anulada pelo Poder Judiciário, devendo tal condição constar expressamente dos editais de licitação.

- 4.3. Como condição para participação no Pregão, a licitante assinalará “sim” ou “não” em campo próprio do sistema eletrônico, relativo às seguintes declarações:
- 4.3.1. Que cumpre os requisitos estabelecidos no artigo 3º da Lei Complementar nº 123, de 2006, estando apta a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49;
- 4.3.1.1. Nos itens exclusivos para participação de microempresas e empresas de pequeno porte, a assinalação do campo “não” impedirá o prosseguimento no certame;
- 4.3.1.2. Nos itens em que a participação não for exclusiva para microempresas e empresas de pequeno porte, a assinalação do campo “não” apenas produzirá o efeito de o licitante não ter direito ao tratamento favorecido previsto na Lei Complementar nº 123, de 2006, mesmo que microempresa, empresa de pequeno porte.
- 4.3.2. Que está ciente e concorda com as condições contidas no Edital e seus anexos;
- 4.3.3. Que cumpre os requisitos para a habilitação definidos no Edital e que a proposta apresentada está em conformidade com as exigências editalícias;
- 4.3.4. Que inexistem fatos impeditivos para sua habilitação no certame, ciente da obrigatoriedade de declarar ocorrências posteriores;
- 4.3.5. Que não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do artigo 7º, XXXIII, da Constituição;
- 4.3.6. Que a proposta foi elaborada de forma independente, nos termos da Instrução Normativa SLTI/MP nº 2, de 16 de setembro de 2009.
- 4.3.7. Que não possui, em sua cadeia produtiva, empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal;
- 4.3.8. Que os serviços são prestados por empresas que comprovem cumprimento de reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social e que atendam às regras de acessibilidade previstas na legislação, conforme disposto no art. 93 da Lei nº 8.213, de 24 de julho de 1991.
- 4.4. **DA VEDAÇÃO ÀS PRÁTICAS DE NEPOTISMO**
- 4.4.1. A licitante melhor classificada deverá apresentar, na habilitação, a declaração de inexistência de fato impeditivo referente à Resolução nº 037/2009-CNMP”, **Anexo IV** do edital, devidamente assinada pelo representante legal da empresa. Não cumprido este item, o Pregoeiro reputará o licitante inabilitado, por falta de condição de participação, contudo sua ausência ou falha não gera inabilitação imediata, podendo ser suprida mediante diligência prevista no item 11 deste edital.
- 4.5. A declaração falsa relativa ao cumprimento de qualquer condição sujeitará o licitante às sanções previstas em lei e neste Edital.

5. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

- 5.1. Os licitantes encaminharão, exclusivamente por meio do sistema, concomitantemente com os documentos de habilitação exigidos no edital, proposta com a descrição do objeto ofertado e o preço, até a data e o horário estabelecidos para abertura da sessão pública, quando, então, encerrar-se-á automaticamente a etapa de envio dessa documentação.
- 5.2. O envio da proposta, acompanhada dos documentos de habilitação exigidos neste Edital, ocorrerá por meio de chave de acesso e senha.
- 5.3. Os licitantes poderão deixar de apresentar os documentos de habilitação que constem do SICAF, assegurado aos demais licitantes o direito de acesso aos dados constantes dos sistemas.

- 5.4. As Microempresas e Empresas de Pequeno Porte deverão encaminhar a documentação de habilitação, ainda que haja alguma restrição de regularidade fiscal e trabalhista, nos termos do art. 43, § 1º da LC nº 123, de 2006.
- 5.5. Incumbirá ao licitante acompanhar as operações no sistema eletrônico durante a sessão pública do Pregão, ficando responsável pelo ônus decorrente da perda de negócios, diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão.
- 5.6. Até a abertura da sessão pública, os licitantes poderão retirar ou substituir a proposta e os documentos de habilitação anteriormente inseridos no sistema;
- 5.7. Não será estabelecida, nessa etapa do certame, ordem de classificação entre as propostas apresentadas, o que somente ocorrerá após a realização dos procedimentos de negociação e julgamento da proposta.
- 5.8. Os documentos que compõem a proposta e a habilitação do licitante melhor classificado somente serão disponibilizados para avaliação do pregoeiro e para acesso público após o encerramento do envio de lances.

6. DO PREENCHIMENTO DA PROPOSTA

- 6.1. O licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, dos seguintes campos:
 - 6.1.1. **Valor unitário e total do item e do grupo (considerando o campo “Unidade de Fornecimento” do *compras governamentais*);**
 - 6.1.2. Marca;
 - 6.1.3. Fabricante;
 - 6.1.4. Descrição detalhada do objeto, contendo as informações similares à especificação do Termo de Referência: indicando, no que for aplicável, o modelo, prazo de validade ou de garantia, número do registro ou inscrição do bem no órgão competente, quando for o caso;
- 6.2. Todas as especificações do objeto contidas na proposta vinculam a Contratada.
- 6.3. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente no fornecimento dos bens.
- 6.4. Os preços ofertados, tanto na proposta inicial, quanto na etapa de lances, serão de exclusiva responsabilidade do licitante, não lhe assistindo o direito de pleitear qualquer alteração, sob alegação de erro, omissão ou qualquer outro pretexto.
- 6.5. O prazo de validade da proposta não será inferior a **60 (sessenta) dias**, a contar da data de sua apresentação.
 - 6.5.1. Esse prazo fica suspenso pelo tempo necessário à conclusão de diligências e no caso de interposição de recurso, inclusive até seu julgamento;

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

- 7.1. A abertura da presente licitação dar-se-á em sessão pública, por meio de sistema eletrônico, na data, horário e local indicados neste Edital.
- 7.2. O Pregoeiro verificará as propostas apresentadas, desclassificando desde logo aquelas que não estejam em conformidade com os requisitos estabelecidos neste Edital, contenham vícios insanáveis ou não apresentem as especificações técnicas exigidas no Termo de Referência.
 - 7.2.1. Também será desclassificada a proposta que identifique o licitante.
 - 7.2.2. A desclassificação será sempre fundamentada e registrada no sistema, com acompanhamento em tempo real por todos os participantes.
 - 7.2.3. A não desclassificação da proposta não impede o seu julgamento definitivo em sentido contrário, levado a efeito na fase de aceitação.
- 7.3. O sistema ordenará automaticamente as propostas classificadas, sendo que somente estas participarão da fase de lances.
- 7.4. O sistema disponibilizará campo próprio para troca de mensagens entre o Pregoeiro e os licitantes.

- 7.5. Iniciada a etapa competitiva, os licitantes deverão encaminhar lances exclusivamente por meio do sistema eletrônico, sendo imediatamente informados do seu recebimento e do valor consignado no registro.
- 7.6. Os registros dos valores dos lances devem ser realizados considerando o indicado no campo “**Unidade de Fornecimento**” do *compras governamentais*, sem prejuízo ao critério de classificação do certame;
- 7.7. Os licitantes poderão oferecer lances sucessivos, observando o horário fixado para abertura da sessão e as regras estabelecidas no Edital.
- 7.8. O licitante somente poderá oferecer lance de valor inferior ao último por ele ofertado e registrado pelo sistema.
- 7.9. **O intervalo mínimo de diferença de valores entre os lances**, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta **deverá ser de 5% (cinco) por cento**.
- 7.10. O intervalo entre os lances enviados pelo mesmo licitante não poderá ser inferior a vinte (20) segundos e o intervalo entre lances não poderá ser inferior a três (3) segundos, sob pena de serem automaticamente descartados pelo sistema os respectivos lances.
- 7.11. Cada lance é de exclusiva responsabilidade do licitante, não lhe cabendo o direito a pleitear alteração ou desistência.
- 7.12. Será adotado para o envio de lances no pregão eletrônico o **modo de disputa “aberto”**, em que os licitantes apresentarão lances públicos e sucessivos, com prorrogações.
- 7.13. A etapa de lances da sessão pública terá duração de dez minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos dois minutos do período de duração da sessão pública.
- 7.14. A prorrogação automática da etapa de lances, de que trata o item anterior, será de dois minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários.
- 7.15. Não havendo novos lances na forma estabelecida nos itens anteriores, a sessão pública encerrar-se-á automaticamente.
- 7.16. Encerrada a fase competitiva sem que haja a prorrogação automática pelo sistema, poderá o pregoeiro, assessorado pela equipe de apoio, justificadamente, admitir o reinício da sessão pública de lances, em prol da consecução do melhor preço.
- 7.17. Em caso de falha no sistema, os lances em desacordo com os subitens anteriores deverão ser desconsiderados pelo pregoeiro, devendo a ocorrência ser comunicada imediatamente à Secretaria de Gestão do Ministério da Economia;
 - 7.17.1. Na hipótese do subitem anterior, a ocorrência será registrada em campo próprio do sistema.
- 7.18. Não serão aceitos dois ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado em primeiro lugar.
- 7.19. Durante o transcurso da sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado, vedada a identificação do licitante.
- 7.20. No caso de desconexão com o Pregoeiro, no decorrer da etapa competitiva do Pregão, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances.
- 7.21. 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.
- 7.22. O Critério de julgamento adotado será o **menor preço**, conforme definido neste Edital e seus anexos.
- 7.23. Caso o licitante não apresente lances, concorrerá com o valor de sua proposta.
- 7.24. Em relação a itens não exclusivos para participação de microempresas e empresas de pequeno porte, uma vez encerrada a etapa de lances, será efetivada a verificação automática, junto à Receita Federal, do porte da entidade empresarial. O sistema identificará em coluna própria as microempresas e empresas de pequeno porte participantes, procedendo à comparação com os valores da primeira colocada, se esta for empresa de maior porte, assim como das demais classificadas, para o fim de aplicar-se o

- disposto nos arts. 44 e 45 da LC nº 123, de 2006, regulamentada pelo Decreto nº 8.538, de 2015.
- 7.25. Nessas condições, as propostas de microempresas e empresas de pequeno porte que se encontrarem na faixa de até 5% (cinco por cento) acima da melhor proposta ou melhor lance serão consideradas empatadas com a primeira colocada.
 - 7.26. A melhor classificada nos termos do item anterior terá o direito de encaminhar uma última oferta para desempate, obrigatoriamente em valor inferior ao da primeira colocada, no prazo de 5 (cinco) minutos controlados pelo sistema, contados após a comunicação automática para tanto.
 - 7.27. Caso a microempresa ou a empresa de pequeno porte melhor classificada desista ou não se manifeste no prazo estabelecido, serão convocadas as demais licitantes microempresa e empresa de pequeno porte que se encontrem naquele intervalo de 5% (cinco por cento), na ordem de classificação, para o exercício do mesmo direito, no prazo estabelecido no subitem anterior.
 - 7.28. No caso de equivalência dos valores apresentados pelas microempresas e empresas de pequeno porte que se encontrem nos intervalos estabelecidos nos subitens anteriores, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta.
 - 7.29. A ordem de apresentação pelos licitantes é utilizada como um dos critérios de classificação, de maneira que só poderá haver empate entre propostas iguais (não seguidas de lances).
 - 7.30. **Havendo eventual empate** entre propostas ou lances, o critério de desempate será aquele previsto no art. 3º, § 2º, da Lei nº 8.666, de 1993, assegurando-se a preferência, sucessivamente, aos bens produzidos:
 - 7.30.1. No país;
 - 7.30.2. Por empresas brasileiras;
 - 7.30.3. Por empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País;
 - 7.30.4. Por empresas que comprovem cumprimento de reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social e que atendam às regras de acessibilidade previstas na legislação.
 - 7.31. **Persistindo o empate**, a proposta vencedora será sorteada pelo sistema eletrônico dentre as propostas empatadas.
 - 7.32. Encerrada a etapa de envio de lances da sessão pública, o pregoeiro deverá encaminhar, pelo sistema eletrônico, contraproposta ao licitante que tenha apresentado o melhor preço, para que seja obtida melhor proposta, vedada a negociação em condições diferentes das previstas neste Edital.
 - 7.32.1. A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes.
 - 7.32.2. O pregoeiro solicitará ao licitante melhor classificado que, no prazo de **até 02 (duas) horas**, envie a proposta adequada ao último lance ofertado após a negociação realizada, acompanhada, se for o caso, dos documentos complementares, quando necessários à confirmação daqueles exigidos neste Edital e já apresentados.
 - 7.33. Após a negociação do preço, o Pregoeiro iniciará a fase de aceitação e julgamento da proposta.

8. DA ACEITABILIDADE DA PROPOSTA VENCEDORA.

- 8.1. Como condição prévia à aceitação da proposta, caso o licitante detentor da proposta classificada em primeiro lugar tenha usufruído do tratamento diferenciado previsto nos artigos 44 e 45 da Lei Complementar nº 123, de 2006, o Pregoeiro deverá consultar o Portal da Transparência do Governo Federal, seção “Despesas – Gastos Diretos do Governo – Favorecido (pessoas físicas, empresas e outros)”, para verificar se o somatório dos valores das ordens bancárias por ele recebidas, no exercício anterior, extrapola o limite previsto no artigo 3º, inciso II, da Lei Complementar nº 123, de 2006, ou o limite proporcional de que trata o artigo 3º, § 2º, do mesmo diploma, em caso de início de atividade no exercício considerado.

- 8.1.1. Para a microempresa ou empresa de pequeno porte, a consulta também abrangerá o exercício corrente, para verificar se o somatório dos valores das ordens bancárias por ela recebidas, até o mês anterior ao da sessão pública da licitação, extrapola os limites acima referidos, acrescidos do percentual de 20% (vinte por cento) de que trata o artigo 3º, §§ 9º-A e 12, da Lei Complementar nº 123, de 2006.
- 8.1.2. Constatada a ocorrência de qualquer das situações de extrapolação do limite legal, o Pregoeiro deverá indeferir a aplicação do tratamento diferenciado em favor do licitante, conforme artigo 3º, §§ 9º, 9º-A, 10 e 12, da Lei Complementar nº 123, de 2006, com a consequente recusa do lance de desempate, sem prejuízo das penalidades incidentes (ver TCU, Ac. n. 1.793/2011 – Plenário).
- 8.2. Encerrada a etapa de negociação, o pregoeiro examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao máximo estipulado para contratação neste Edital e em seus anexos, observado o disposto no parágrafo único do art. 7º e no § 9º do art. 26 do Decreto n.º 10.024/2019.
- 8.3. Será desclassificada a proposta ou o lance vencedor, apresentar preço final superior ao preço máximo fixado (Acórdão nº 1455/2018 -TCU - Plenário), ou que apresentar preço manifestamente inexequível.
 - 8.3.1. Considera-se inexequível a proposta que apresente preços global ou unitários simbólicos, irrisórios ou de valor zero, incompatíveis com os preços dos insumos e salários de mercado, acrescidos dos respectivos encargos, ainda que o ato convocatório da licitação não tenha estabelecido limites mínimos, exceto quando se referirem a materiais e instalações de propriedade do próprio licitante, para os quais ele renuncie a parcela ou à totalidade da remuneração.
 - 8.3.2. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderá ser efetuada diligência para efeito de comprovação de sua exequibilidade, podendo ser adotado, dentre outros, os seguintes procedimentos, sem prejuízo de outras solicitações:
 - I. Questionamentos junto à proponente para a apresentação de justificativas e comprovações em relação aos custos com indícios de inexequibilidade;
 - II. Pesquisas em órgãos públicos ou empresas privadas;
 - III. Verificação de outros contratos que o proponente mantenha com a Administração ou com a iniciativa privada;
 - IV. Pesquisa de preço com fornecedores dos insumos utilizados, tais como: atacadistas, lojas de suprimentos, supermercados e fabricantes;
 - V. Verificação de notas fiscais dos produtos adquiridos pelo proponente;
 - VI. Planilha de Formação de Custos do item em análise, acompanhada de documentos comprobatórios dos custos informados;
- 8.4. Na hipótese de necessidade de suspensão da sessão pública para a realização de diligências, com vistas ao saneamento das propostas, a sessão pública somente poderá ser reiniciada mediante aviso prévio no sistema com, no mínimo, vinte e quatro horas de antecedência, e a ocorrência será registrada em ata;
- 8.5. O Pregoeiro poderá convocar o licitante para enviar documento digital complementar, por meio de funcionalidade disponível no sistema, no prazo de **até 02 (duas) horas**, sob pena de não aceitação da proposta.
 - 8.5.1. O prazo estabelecido poderá ser prorrogado pelo Pregoeiro por solicitação escrita e justificada do licitante, formulada antes de findo o prazo, e formalmente aceita pelo Pregoeiro.
 - 8.5.2. Dentre os documentos passíveis de solicitação pelo Pregoeiro, destacam-se os que contenham as características do material ofertado, tais como marca, modelo, tipo, fabricante e procedência, além de outras informações pertinentes, a exemplo de catálogos, folhetos ou propostas, encaminhados por meio eletrônico, ou, se for o caso, por outro meio e prazo indicados pelo Pregoeiro, sem prejuízo do seu ulterior envio pelo sistema eletrônico, sob pena de não aceitação da proposta-

- 8.6. Para fins de análise da proposta quanto ao cumprimento das especificações do objeto, poderá ser colhida a manifestação escrita do setor requisitante do serviço ou da área especializada no objeto.
- 8.7. Se a proposta ou lance vencedor for desclassificado, o Pregoeiro examinará a proposta ou lance subsequente, e, assim sucessivamente, na ordem de classificação.
- 8.8. Havendo necessidade, o Pregoeiro suspenderá a sessão, informando no “chat” a nova data e horário para a sua continuidade.
- 8.9. O Pregoeiro poderá encaminhar, por meio do sistema eletrônico, contraproposta ao licitante que apresentou o lance mais vantajoso, com o fim de negociar a obtenção de melhor preço, vedada a negociação em condições diversas das previstas neste Edital.
- 8.9.1. Também nas hipóteses em que o Pregoeiro não aceitar a proposta e passar à subsequente, poderá negociar com o licitante para que seja obtido preço melhor.
- 8.9.2. A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes.
- 8.10. Nos itens não exclusivos para a participação de microempresas e empresas de pequeno porte, sempre que a proposta não for aceita, e antes de o Pregoeiro passar à subsequente, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos artigos 44 e 45 da LC nº 123, de 2006, seguindo-se a disciplina antes estabelecida, se for o caso.
- 8.11. **Serão desclassificadas as propostas que apresentarem preços superiores aos definidos no critério de aceitabilidade do preço global e por item:**
- 8.11.1. O CRITÉRIO DE ACEITABILIDADE DO PREÇO UNITÁRIO da proposta cotada pelos licitantes será de no máximo o valor orçado pela Administração para **cada item**, conforme o previsto no quadro do item 3 do Termo de Referência, na coluna “**Preço Unitário Máximo**”:
- 8.11.2. O CRITÉRIO DE ACEITABILIDADE DO PREÇO GLOBAL da proposta cotada pelos licitantes será de no máximo o valor orçado pela Administração para **o total do grupo**, conforme o previsto no quadro do item 3 do Termo de Referência, na linha “**Valor Total Máximo do Grupo**”:
- 8.12. **DO CATÁLOGO OU PROSPECTO (Para os itens 01 a 03):** da licitante cuja proposta apresentar o menor preço após conclusão fase de lances, **poderão** ser solicitados **CATÁLOGOS, PROSPECTOS** do(s) respectivo(s) item(ns) em análise, nas condições descritas no item 12.1 deste edital, informando as especificações técnicas, indicação do fabricante, marca modelo e referência, de acordo com o objeto:
- 8.12.1. O catálogo ou prospecto deverá ser enviado após convocação;
- 8.12.2. A Área Técnica verificará a conformidade do produto ofertado com as especificações constantes no Termo de Referência;
- 8.12.3. A necessidade do catálogo ou prospecto se verificará nos casos onde houver dúvidas quanto as especificações do produto ofertado pelo licitante e essas informações não puderem ser verificadas em endereços eletrônicos;
- 8.12.4. A proposta será desclassificada se:
- 8.12.4.1. Ficar demonstrado pelos catálogos ou prospectos que as especificações não atendem aos requisitos mínimos exigidos no termo de referência;
- 8.12.4.2. Não for enviado, quando solicitado, o catálogo ou prospecto para comprovar as especificações dispostas na proposta do licitante;
- 8.12.4.3. O catálogo ou prospecto enviado não comprovar as especificações dispostas na proposta do licitante;
- 8.12.4.4. Não existirem no catálogo ou prospecto as informações técnicas relevantes e/ou marca e referência do produto cotado.

- 8.13. **DOS DOCUMENTOS:** Em relação aos itens de 1 a 4, a licitante deverá apresentar junto com a proposta a lista de **PART NUMBERS** do fabricante e suas respectivas quantidades necessárias para atender as características técnicas solicitadas neste edital; **Uma vez o Departamento de Informática justifica que o "partnumber identifica especificamente o equipamento, trazendo além da marca, o modelo e a versão do produto, de forma que é possível verifica-lo a partir de datasheets (documento oficial do fabricante informando as especificações do produto e suas demais características técnicas) do equipamento, garantindo que o que foi ofertado deve ser o que será entregue."**
- 8.14. Irregularidades formais que evidenciem lapso isento de má-fé e que não afetem o conteúdo da proposta, não constituirão, por si, motivo de desclassificação, podendo o pregoeiro sanar erros ou falhas que não alterem a substância da proposta, dos documentos e sua validade jurídica, mediante despacho fundamentado, registrado devidamente em ata.
- 8.15. Posteriormente não serão admitidas alegações de enganos, erros ou distrações na elaboração das propostas de preços como justificativas de solicitação de quaisquer acréscimos, de reequilíbrio econômico-financeiro da proposta, de indenizações, ou ressarcimentos de qualquer natureza. Os licitantes deverão arcar com todos os custos decorrentes da elaboração e apresentação de suas propostas.
- 8.16. Encerrada a análise quanto à aceitação da proposta, o pregoeiro verificará a habilitação do licitante, observado o disposto neste Edital.

9. DA HABILITAÇÃO

- 9.1. Como condição prévia ao exame da documentação de habilitação do licitante detentor da proposta classificada em primeiro lugar, o Pregoeiro verificará o eventual descumprimento das condições de participação, observando o item 4, na íntegra, e ainda quanto à existência de sanção que impeça a participação no certame ou na futura contratação, mediante declarações ou consultas aos cadastros abaixo, conforme o caso, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:
- 9.1.1. SICAF;
- 9.1.2. Consulta Consolidada de Pessoa Jurídica do Tribunal de Contas da União (<https://certidoes-apf.apps.tcu.gov.br/>), recomendação do TCU (Acórdão nº 1.793/2011 – Plenário).
- 9.1.3. A consulta aos cadastros será realizada em nome da empresa licitante e também de seu sócio majoritário, por força do artigo 12 da Lei nº 8.429, de 1992, que prevê, dentre as sanções impostas ao responsável pela prática de ato de improbidade administrativa, a proibição de contratar com o Poder Público, inclusive por intermédio de pessoa jurídica da qual seja sócio majoritário.
- 9.1.3.1. Caso conste na Consulta de Situação do Fornecedor a existência de Ocorrências Impeditivas Indiretas, o gestor diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas.
- 9.1.3.2. A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros.
- 9.1.3.3. O licitante será convocado para manifestação previamente à sua desclassificação.
- 9.1.4. Constatada a existência de sanção ou outro impedimento de licitar ou contratar com a Administração, o Pregoeiro reputará o licitante inabilitado, por falta de condição de participação.
- 9.1.5. No caso de inabilitação, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos arts. 44 e 45 da Lei Complementar nº 123, de 2006, seguindo-se a disciplina antes estabelecida para aceitação da proposta subsequente.

- 9.2. Caso atendidas as condições de participação, a habilitação do licitante será verificada por meio do SICAF, nos documentos por ele abrangidos em relação à habilitação jurídica, à regularidade fiscal e trabalhista, à qualificação econômica financeira e habilitação técnica, conforme o disposto na Instrução Normativa SEGES/MP nº 03, de 2018.
- 9.2.1. O interessado, para efeitos de habilitação prevista na Instrução Normativa SEGES/MP nº 03, de 2018 mediante utilização do sistema, deverá atender às condições exigidas no cadastramento no SICAF até o terceiro dia útil anterior à data prevista para recebimento das propostas;
- 9.2.2. É dever do licitante atualizar previamente as comprovações constantes do SICAF para que estejam vigentes na data da abertura da sessão pública, ou encaminhar, em conjunto com a apresentação da proposta, a respectiva documentação atualizada.
- 9.2.3. O descumprimento do subitem acima implicará a inabilitação do licitante, exceto se a consulta aos sítios eletrônicos oficiais emissores de certidões feita pelo Pregoeiro lograr êxito em encontrar a(s) certidão(ões) válida(s), conforme art. 43, §3º, do Decreto 10.024, de 2019.
- 9.3. Havendo a necessidade de envio de documentos de habilitação complementares, necessários à confirmação daqueles exigidos neste Edital e já apresentados, o licitante será convocado a encaminhá-los, em formato digital, via sistema, no prazo de **até 02 (duas) horas**, sob pena de inabilitação.
- 9.4. Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante apresentação dos documentos originais não-digitais quando houver dúvida em relação à integridade do documento digital.
- 9.5. Não serão aceitos documentos de habilitação com indicação de CNPJ/CPF diferentes, salvo aqueles legalmente permitidos.
- 9.6. Se o licitante for a matriz, todos os documentos deverão estar em nome da matriz, e se o licitante for a filial, todos os documentos deverão estar em nome da filial, exceto aqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.
- 9.6.1. Serão aceitos registros de CNPJ de licitante matriz e filial com diferenças de números de documentos pertinentes ao CND e ao CRF/FGTS, quando for comprovada a centralização do recolhimento dessas contribuições.
- 9.7. Expirada a validade de certidão entre a data de sua apresentação e a data da análise da habilitação, a licitante deverá enviar comprovante de validade, para complementar a informação, no prazo de até duas horas a partir da solicitação do pregoeiro e observado o item 9.3 do edital;
- 9.8. **Ressalvado o disposto no item 5.3, os licitantes deverão encaminhar**, nos termos deste Edital, a documentação relacionada nos itens a seguir, para fins de habilitação e condição de participação:
- 9.9. **Habilitação jurídica:**
- 9.9.1. No caso de empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;
- 9.9.2. Em se tratando de microempreendedor individual – MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio www.portaldoempreendedor.gov.br;
- 9.9.3. No caso de sociedade empresária ou empresa individual de responsabilidade limitada - EIRELI: ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado na Junta Comercial da respectiva sede, acompanhado de documento comprobatório de seus administradores;
- 9.9.4. Inscrição no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz, no caso de ser a participante sucursal, filial ou agência;

- 9.9.5. No caso de sociedade simples: inscrição do ato constitutivo no Registro Civil das Pessoas Jurídicas do local de sua sede, acompanhada de prova da indicação dos seus administradores;
- 9.9.6. No caso de cooperativa: ata de fundação e estatuto social em vigor, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, bem como o registro de que trata o art. 107 da Lei nº 5.764, de 1971;
- 9.9.7. No caso de empresa ou sociedade estrangeira em funcionamento no País: decreto de autorização;
- 9.9.8. Os documentos acima deverão estar acompanhados de todas as alterações ou da consolidação respectiva;
- 9.10. **Regularidade fiscal e trabalhista:**
- 9.10.1. Prova de inscrição no **Cadastro Nacional de Pessoas Jurídicas**;
- 9.10.2. prova de regularidade fiscal perante a **Fazenda Nacional**, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02/10/2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.
- 9.10.3. Prova de regularidade com o **Fundo de Garantia do Tempo de Serviço (FGTS)**;
- 9.10.4. Prova de inexistência de débitos inadimplidos perante a **justiça do trabalho**, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943;
- 9.10.5. Prova de regularidade com a **Fazenda Estadual** do domicílio ou sede do licitante;
- 9.10.6. Prova de regularidade com a **Fazenda Municipal** do domicílio ou sede do licitante;
- 9.10.7. Caso o licitante seja considerado isento dos tributos estaduais relacionados ao objeto licitatório, deverá comprovar tal condição mediante declaração da Fazenda Estadual do seu domicílio ou sede, ou outra equivalente, na forma da lei;
- 9.10.8. Caso o licitante detentor do menor preço seja qualificado como microempresa ou empresa de pequeno porte deverá apresentar toda a documentação exigida para efeito de comprovação de regularidade fiscal, mesmo que esta apresente alguma restrição, sob pena de inabilitação.
- 9.10.8.1. A licitante melhor classificada deverá, também, apresentar a documentação de regularidade fiscal das microempresas e/ou empresas de pequeno porte que serão subcontratadas no decorrer da execução do contrato, ainda que exista alguma restrição, aplicando-se o prazo de regularização previsto no art. 4º, §1º do Decreto nº 8.538, de 2015.
- 9.11. **Qualificação Econômico-Financeira.**
- 9.11.1. **Certidão negativa de falência, concordata ou recuperação judicial/extrajudicial** expedida pelo distribuidor da sede da pessoa jurídica, datada de até 90 (noventa) dias anteriores à data da abertura da sessão;
- 9.11.1.1. **No caso de recuperação judicial a licitante deve comprovar a aprovação do plano de recuperação judicial.**
- 9.12. **Qualificação Técnica**
- 9.12.1. **Atestado de capacidade técnico-operacional**, pelo menos 1 (um) atestado **eu-4 (uma) declaração de capacidade técnica** em nome da licitante, fornecidos por pessoa jurídica de direito público ou privado, onde comprove que a licitante tenha prestado ou esteja prestando, a contento, serviços e objetos descritos no item 3 do Termo de Referência **(Quanto a instalação a empresa deve ter instalado e configurado pelo menos 1 de cada dos equipamentos e 1 sistema de gerência de: 54 equipamentos de pequeno porte (item 1), 8 equipamentos de médio porte (item**

2) e 1 concentrador (item 3). Quanto ao treinamento, que este tenha sido ministrado em uma carga mínima de 8 horas para uma turma de 3 pessoas. Este cálculo levou em consideração as contratações similares realizadas). O atestado emitido por pessoa jurídica de direito privado deverá estar com firma reconhecida;

9.12.1.1. O atestado de capacidade técnico-operacional referido no item 9.1.2, ~~ou a declaração~~, deverá conter os seguintes elementos:

a) Nome do órgão ou empresa responsável pela emissão do atestado, com o CNPJ, inscrição estadual, endereço completo, o período de execução dos serviços e o número do contrato;

~~b) Manifestação acerca do conteúdo e da qualidade dos serviços prestados, atestando que os serviços foram cumpridos satisfatoriamente e que não consta dos arquivos da contratante nenhum registro desabonador de aspectos comerciais ou técnicos da CONTRATADA;~~

b) Manifestação acerca do conteúdo e da qualidade da solução apresentada, atestando que os produtos foram entregues de acordo com as especificações e os serviços foram cumpridos satisfatoriamente

c) Identificação do responsável pela emissão do atestado, com nome, função e telefone para solicitação de informações adicionais.

9.12.1.2. Para efeitos de atendimento do item 9.1.2, o(s) atestado(s) de capacidade técnico-operacional ou a(s) declaração(ões), deverá(ão) atender os parâmetros mínimos listados na tabela abaixo:

Itens	Capacidade
1 a 4	Ter fornecido equipamentos compatíveis (na proporção de no mínimo 40% de toda a solução descrita em cada item) em características com os objetos da presente licitação.
5	Haver assegurado instalação/configuração de equipamentos compatíveis (na proporção de no mínimo 40% de toda a solução descrita em cada item) em características com os objetos da presente licitação.
6	Haver efetuado treinamento incluindo instalação, configuração, troubleshoot, monitoramento e gerenciamento para os itens 1 a 4 da Solução de Firewall/SD (na proporção de no mínimo 40% deste item)

9.12.1.3. De acordo com os acórdãos 2.882/2008 e 2.646/2015 do TCU, será aceita a somatória de atestados para fim de qualificação técnica, desde que limitados a 3 atestados por item.

9.12.1.4. Não serão considerados atestados emitidos por distribuidor ou fabricante dos equipamentos cotados, em favor da licitante. Em qualquer caso o atestado deve ser emitido pela empresa, órgão ou entidade pública que contratou os produtos/serviços (cliente final) em favor da licitante.

9.12.1.5. Em atendimento ao Acórdão TCU 1058-13-14-P, não estando o atestado com a firma reconhecida, o(a) Pregoeiro(a) deverá solicitar em diligência o devido reconhecimento da firma.

9.12.1.6. É **facultado** ao pregoeiro realizar diligências a fim de complementar ou comprovar os documentos apresentados;

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

9.12.1.8. Poderá ser admitida, para fins de comprovação de quantitativo mínimo do serviço, a apresentação de diferentes atestados de serviços executados de forma concomitante, pois essa situação se equivale, para fins de comprovação de

capacidade técnico-operacional, a uma única contratação, nos termos do item 10.9 do Anexo VII-A da IN SEGES/MPDG n. 5/2017.

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

9.13. **Declaração de inexistência de fato impeditivo** referente à Resolução nº 037/2009-CNMP”, **Anexo IV** do edital, devidamente assinada pelo representante legal da empresa, nos termos do item 4.4.1.

9.13.1. **A ausência ou falha nesta declaração não gera inabilitação imediata, podendo ser suprida mediante diligência prevista no item 11 deste edital.**

9.14. Tratando-se de licitantes reunidos em consórcio, serão observadas as seguintes exigências:

9.14.1. Comprovação da existência de compromisso público ou particular de constituição de consórcio, subscrito pelas empresas que dele participarão, com indicação da empresa-líder, que deverá possuir amplos poderes para representar os consorciadas no procedimento licitatório e no instrumento contratual, receber e dar quitação, responder administrativa e judicialmente, inclusive receber notificação, intimação e citação;

9.14.2. Apresentação da documentação de habilitação especificada no edital por empresa consorciada;

9.14.3. Comprovação da capacidade técnica do consórcio pelo somatório dos quantitativos de cada consorciado, na forma estabelecida neste edital;

9.14.4. Responsabilidade solidária das empresas consorciadas pelas obrigações do consórcio, nas fases de licitação e durante a vigência do contrato;

9.14.5. Obrigatoriedade de liderança por empresa brasileira no consórcio formado por empresas brasileiras e estrangeiras;

9.14.6. Constituição e registro do consórcio antes da celebração do contrato; e

9.14.7. Proibição de participação de empresa consorciada, na mesma licitação, por intermédio de mais de um consórcio ou isoladamente.

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

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

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

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

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

- 9.19. Havendo necessidade de analisar minuciosamente os documentos exigidos, o Pregoeiro suspenderá a sessão, informando no “chat” a nova data e horário para a continuidade da mesma.
- 9.20. Será inabilitado o licitante que não comprovar sua habilitação, seja por não apresentar quaisquer dos documentos exigidos, ou apresentá-los em desacordo com o estabelecido neste Edital.
- 9.21. Nos itens não exclusivos a microempresas e empresas de pequeno porte, em havendo inabilitação, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos artigos 44 e 45 da LC nº 123, de 2006, seguindo-se a disciplina antes estabelecida para aceitação da proposta subsequente.
- 9.22. Constatado o atendimento às exigências de habilitação fixadas no Edital, o licitante será declarado vencedor pelo menor **preço global do grupo**.

10. DO ENCAMINHAMENTO DA PROPOSTA VENCEDORA

- 10.1. A proposta final do licitante declarado vencedor deverá ser encaminhada no prazo de **até 02 (duas) horas**, a contar da solicitação do Pregoeiro no sistema eletrônico e deverá:
 - 10.1.1. Ser redigida em língua portuguesa, datilografada ou digitada, em uma via, sem emendas, rasuras, entrelinhas ou ressalvas, devendo a última folha ser assinada e as demais rubricadas pelo licitante ou seu representante legal, ou assinada via certificação eletrônica.
 - 10.1.2. Conter a indicação do banco, número da conta e agência do licitante vencedor, para fins de pagamento.
 - 10.1.3. E-mail, endereço e telefone do licitante;
- 10.2. A proposta final deverá ser documentada nos autos e será levada em consideração no decorrer da execução do contrato e aplicação de eventual sanção à Contratada, se for o caso.
 - 10.2.1. Todas as especificações do objeto contidas na proposta, tais como marca, modelo, tipo, fabricante, procedência e garantia, vinculam a Contratada.
- 10.3. Os preços deverão ser expressos em moeda corrente nacional, o valor unitário em algarismos e o valor global em algarismos e por extenso (art. 5º da Lei nº 8.666/93).
 - 10.3.1. Ocorrendo divergência entre os preços unitários e o preço global, prevalecerão os primeiros; no caso de divergência entre os valores numéricos e os valores expressos por extenso, prevalecerão estes últimos.
- 10.4. A oferta deverá ser firme e precisa, limitada, rigorosamente, ao objeto deste Edital, sem conter alternativas de preço ou de qualquer outra condição que induza o julgamento a mais de um resultado, sob pena de desclassificação.
- 10.5. A proposta deverá obedecer aos termos deste Edital e seus Anexos, não sendo considerada aquela que não corresponda às especificações ali contidas ou que estabeleça vínculo à proposta de outro licitante.
- 10.6. As propostas que contenham a descrição do objeto, o valor e os documentos complementares estarão disponíveis na internet, após a homologação.
- 10.7. A ausência ou falha no encaminhamento da **proposta vencedora** não gera desclassificação imediata, podendo ser suprida mediante diligência prevista no item 11 deste edital.

11. DA DILIGÊNCIA

- 11.1. Quando solicitado pelo pregoeiro, a licitante deverá enviar em **até 02 (duas) hora após a solicitação**, por meio da opção “Enviar Anexo” do *Sistema Comprasnet* e na sua impossibilidade através de email pregao@mppa.mp.br ou fax (91) 4006-3503, os documentos, inclusive catálogo e/ou prospectos, que a pregoeira entenda necessários para esclarecer ou complementar a instrução do processo.
 - 11.1.1. O prazo definido no item 11.1 poderá ser prorrogado a critério do Pregoeiro(a), que informará o tempo de prorrogação no *Sistema Comprasnet*.
 - 11.1.2. A documentação enviada fora do prazo ou não enviada ao(à) Pregoeiro(a) poderá ensejar a desclassificação ou inabilitação da empresa, se a referida documentação era essencial para o esclarecimento ou complemento da instrução do processo.

12. DA REABERTURA DA SESSÃO PÚBLICA

- 12.1. A sessão pública poderá ser reaberta:
 - 12.1.1. Nas hipóteses de provimento de recurso que leve à anulação de atos anteriores à realização da sessão pública precedente ou em que seja anulada a própria sessão pública, situação em que serão repetidos os atos anulados e os que dele dependam.
 - 12.1.2. Quando houver erro na aceitação do preço melhor classificado ou quando o licitante declarado vencedor não assinar o contrato, não retirar o instrumento equivalente ou não comprovar a regularização fiscal e trabalhista, nos termos do art. 43, §1º da LC nº 123/2006. Nessas hipóteses, serão adotados os procedimentos imediatamente posteriores ao encerramento da etapa de lances.
- 12.2. Todos os licitantes remanescentes deverão ser convocados para acompanhar a sessão reaberta.
 - 12.2.1. A convocação se dará por meio do sistema eletrônico (“chat”), e-mail, ou, ainda, fac-símile, de acordo com a fase do procedimento licitatório.
 - 12.2.2. A convocação feita por e-mail ou fac-símile dar-se-á de acordo com os dados contidos no SICAF, sendo responsabilidade do licitante manter seus dados cadastrais atualizados.

13. DOS RECURSOS

- 13.1. O Pregoeiro declarará o vencedor e, depois de decorrida a fase de regularização fiscal e trabalhista de microempresa ou empresa de pequeno porte, se for o caso, concederá o prazo de no mínimo trinta minutos, para que qualquer licitante manifeste a intenção de recorrer, de forma motivada, isto é, indicando contra quais decisões pretende recorrer e por quais motivos, em campo próprio do sistema.
- 13.2. Havendo quem se manifeste, caberá ao Pregoeiro verificar a tempestividade e a existência de motivação da intenção de recorrer, para decidir se admite ou não o recurso, fundamentadamente.
 - 13.2.1. Nesse momento o Pregoeiro não adentrará no mérito recursal, mas apenas verificará as condições de admissibilidade do recurso.
 - 13.2.1.1. Nota explicativa: no juízo de admissibilidade das intenções de recurso deve ser avaliada tão somente a presença dos pressupostos recursais: sucumbência, tempestividade, legitimidade, interesse e motivação – TCU Ac. 520/2014-Plenário, item 9.5.11.
 - 13.2.2. A falta de manifestação motivada do licitante quanto à intenção de recorrer importará a decadência desse direito.
 - 13.2.3. Uma vez admitido o recurso, o recorrente terá, a partir de então, o prazo de três dias para apresentar as razões, pelo sistema eletrônico, ficando os demais licitantes, desde logo, intimados para, querendo, apresentarem contrarrazões também pelo sistema eletrônico, em outros três dias, que começarão a contar do término do prazo do recorrente, sendo-lhes assegurada vista imediata dos elementos indispensáveis à defesa de seus interesses.
 - 13.2.4. O pregoeiro poderá reconsiderar sua decisão, no prazo de 5 (cinco) dias úteis, ou, nesse mesmo prazo, fazê-lo subir, devidamente informado, devendo, neste caso, a decisão ser proferida dentro do prazo de 5 (cinco) dias úteis, contado do recebimento do recurso, sob pena de responsabilidade.
- 13.3. O acolhimento do recurso invalida tão somente os atos insuscetíveis de aproveitamento.
- 13.4. Os autos do processo permanecerão com vista franqueada aos interessados, no endereço constante neste Edital.

14. DA ADJUDICAÇÃO E HOMOLOGAÇÃO

- 14.1. O objeto da licitação será adjudicado ao licitante declarado vencedor, por ato do Pregoeiro, caso não haja interposição de recurso, ou pela autoridade competente, após a regular decisão dos recursos apresentados.
- 14.2. Após a fase recursal, constatada a regularidade dos atos praticados, a autoridade competente homologará o procedimento licitatório.

15. DA ATA DE REGISTRO DE PREÇOS

- 15.1. Homologado o resultado da licitação, terá o adjudicatário o prazo de **06 (seis) dias**, contados a partir da data de sua convocação, para assinar a Ata de Registro de Preços, cujo prazo de validade encontra-se nela fixado, sob pena de decair do direito à contratação, sem prejuízo das sanções previstas neste Edital.
- 15.2. Alternativamente à convocação para comparecer perante o órgão ou entidade para a assinatura da Ata de Registro de Preços, a Administração poderá encaminhá-la para assinatura, mediante correspondência postal com aviso de recebimento (AR) ou meio eletrônico, para que seja assinada e devolvida no prazo de **06 (seis) dias**, a contar da data de seu recebimento.
- 15.3. O prazo estabelecido no subitem anterior para assinatura da Ata de Registro de Preços poderá ser prorrogado uma única vez, por igual período, quando solicitado pelo(s) licitante(s) vencedor(s), durante o seu transcurso, e desde que devidamente aceito.
- 15.4. Serão formalizadas tantas Atas de Registro de Preços quanto necessárias para o registro de todos os itens constantes no Termo de Referência, com a indicação do licitante vencedor, a descrição do(s) item(ns), as respectivas quantidades, preços registrados e demais condições.
 - 15.4.1. Será incluído na ata, sob a forma de anexo, o registro dos licitantes que aceitarem cotar os bens ou serviços com preços iguais aos do licitante vencedor na sequência da classificação do certame, excluído o percentual referente à margem de preferência, quando o objeto não atender aos requisitos previstos no art. 3º da Lei nº 8.666, de 1993;

16. DO TERMO DE CONTRATO OU INSTRUMENTO EQUIVALENTE

- 16.1. Após a homologação da licitação, em sendo realizada a contratação, será firmado Termo de Contrato ou emitido instrumento equivalente.
- 16.2. O adjudicatário terá o prazo de **06 (seis) dias úteis**, contados a partir da data de sua convocação, para assinar o Termo de Contrato ou aceitar instrumento equivalente, conforme o caso (Nota de Empenho/Carta Contrato/Autorização), sob pena de decair do direito à contratação, sem prejuízo das sanções previstas neste Edital.
 - 16.2.1. Alternativamente à convocação para comparecer perante o órgão ou entidade para a assinatura do Termo de Contrato ou aceite do instrumento equivalente, a Administração poderá encaminhá-lo para assinatura ou aceite da Adjudicatária, mediante correspondência postal com aviso de recebimento (AR) ou meio eletrônico, para que seja assinado ou aceito no prazo de **06 (seis) dias**, a contar da data de seu recebimento.
 - 16.2.2. O prazo previsto no subitem anterior poderá ser prorrogado, por igual período, por solicitação justificada do adjudicatário e aceita pela Administração.
- 16.3. O Aceite da Nota de Empenho ou do instrumento equivalente, emitida à empresa adjudicada, implica no reconhecimento de que:
 - 16.3.1. Referida Nota está substituindo o contrato, aplicando-se à relação de negócios ali estabelecida as disposições da Lei nº 8.666, de 1993;
 - 16.3.2. A contratada se vincula à sua proposta e às previsões contidas no edital e seus anexos;
 - 16.3.3. A contratada reconhece que as hipóteses de rescisão são aquelas previstas nos artigos 77 e 78 da Lei nº 8.666/93 e reconhece os direitos da Administração previstos nos artigos 79 e 80 da mesma Lei.
- 16.4. Previamente à contratação a Administração realizará consulta ao SICAF para identificar possível suspensão temporária de participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas, observado o disposto no art. 29, da Instrução Normativa nº 3, de 26 de abril de 2018, e nos termos do art. 6º, III, da Lei nº 10.522, de 19 de julho de 2002, consulta prévia ao CADIN.

- 16.4.1. Nos casos em que houver necessidade de assinatura do instrumento de contrato, e o fornecedor não estiver inscrito no SICAF, este deverá proceder ao seu cadastramento, sem ônus, antes da contratação.
- 16.4.2. Na hipótese de irregularidade do registro no SICAF, o contratado deverá regularizar a sua situação perante o cadastro no prazo de até 05 (cinco) dias úteis, sob pena de aplicação das penalidades previstas no edital e anexos.
- 16.5. Na assinatura do contrato ou da ata de registro de preços, será exigida a comprovação das condições de habilitação consignadas no edital, que deverão ser mantidas pelo licitante durante a vigência do contrato ou da ata de registro de preços.
- 16.6. Na hipótese de o vencedor da licitação não comprovar as condições de habilitação consignadas no edital ou se recusar a assinar o contrato ou a ata de registro de preços, a Administração, sem prejuízo da aplicação das sanções das demais cominações legais cabíveis a esse licitante, poderá convocar outro licitante, respeitada a ordem de classificação, para, após a comprovação dos requisitos para habilitação, analisada a proposta e eventuais documentos complementares e, feita a negociação, assinar o contrato ou a ata de registro de preços.

17. DO PAGAMENTO

- 17.1. Conforme item 7 do Termo de Referência, anexo deste edital.
- 17.2. Conforme **cláusula quinta da Minuta do Contrato**, anexo deste edital.

18. DOS ACRÉSCIMOS E SUPRESSÕES

- 18.1. Conforme **cláusula sexta da Minuta do Contrato**, anexo deste edital.

19. DO REAJUSTE

- 19.1. Conforme **cláusula sétima da Minuta do Contrato**, anexo deste edital.

20. DOS PRAZOS E CONDIÇÕES DE ENTREGA, RECEBIMENTO DO OBJETO

- 20.1. Conforme item 4 do Termo de Referência, anexo deste edital.
- 20.2. Conforme **cláusula oitava da Minuta do Contrato**, anexo deste edital.

21. DA VIGÊNCIA

- 21.1. Conforme **cláusula nona da Minuta do Contrato**, anexo deste edital.

22. DOS DIREITOS E OBRIGAÇÕES DA CONTRATANTE

- 22.1. Conforme item 5 do Termo de Referência, anexo deste edital.
- 22.2. Conforme **cláusula décima da Minuta do Contrato**, anexo deste edital.

23. DOS DIREITOS E OBRIGAÇÕES DA CONTRATADA

- 23.1. Conforme item 6 do Termo de Referência, anexo deste edital.
- 23.2. Conforme **cláusula décima primeira da Minuta do Contrato**, anexo deste edital.

24. DA GARANTIA DE EXECUÇÃO (somente para contratos a partir de R\$100.000,00)

- 24.1. A **CONTRATADA** deverá prestar a garantia de execução do contrato, **no valor de 5% do contrato**, nos moldes do art. 56 da Lei nº 8.666, de 1993, com validade durante a execução do contrato e 90 (noventa) dias após término da vigência contratual, devendo ser renovada a cada prorrogação, observados ainda os seguintes requisitos:
- 24.1.1. A contratada deverá apresentar, no prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, a critério do órgão contratante, contado da assinatura do contrato, comprovante de prestação de garantia, podendo optar por caução em dinheiro ou títulos da dívida pública, seguro-garantia ou fiança bancária;
- 24.1.2. A garantia, qualquer que seja a modalidade escolhida, assegurará o pagamento de:
- Prejuízos advindos do não cumprimento do objeto do contrato;
 - Prejuízos diretos causados à Administração decorrentes de culpa ou dolo durante a execução do contrato;
 - Multas moratórias e punitivas aplicadas pela Administração à contratada; e

- iv. Obrigações trabalhistas e previdenciárias de qualquer natureza, não adimplidas pela contratada, quando couber.
- 24.1.3. A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados no subitem 24.1.2 acima, observada a legislação que rege a matéria;
- 24.1.4. A garantia em dinheiro deverá ser efetuada no **Banco do Estado do Pará** em conta específica com correção monetária, em favor do contratante;
- 24.1.5. A inobservância do prazo fixado para apresentação da garantia acarretará a aplicação de multa de 0,07% (sete centésimos por cento) do valor do contrato por dia de atraso, observado o máximo de 2% (dois por cento);
- 24.1.6. O atraso superior a 15 (quinze) dias autoriza a Administração a promover a rescisão do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõem os incisos I e II do art. 78 da Lei nº 8.666, de 1993;
- 24.1.7. O garantidor não é parte para figurar em processo administrativo instaurado pelo contratante com o objetivo de apurar prejuízos e/ou aplicar sanções à contratada;
- 24.1.8. A garantia será considerada extinta:
- Com a devolução da apólice, carta-fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração da Administração, mediante termo circunstanciado, de que a contratada cumpriu todas as cláusulas do contrato; e
 - Com o término da vigência do contrato, observado o prazo previsto no subitem 24.1, que poderá, independentemente de sua natureza, ser estendido em caso de ocorrência de sinistro.
- 24.1.9. O contratante executará a garantia na forma prevista na legislação que rege a matéria;
- 24.2. O Contratante fica autorizado a utilizar a garantia para corrigir as imperfeições na execução do Objeto deste contrato ou reparar danos decorrentes da ação ou omissão do Contratado ou de preposto seu ou, ainda, para satisfazer qualquer obrigação resultante ou decorrente de suas ações ou omissões.
- 24.3. O Contratado se obriga a repor, no prazo de 48 (quarenta e oito) horas, o valor da garantia que vier a ser utilizado pelo Contratante.
- 24.4. Em caso de acréscimo ao valor contratual, por meio de termo aditivo, o Contratado fica obrigado a prestar garantia adicional de 5% sobre o valor acrescido;
- 24.4.1. A garantia prestada será retida definitivamente, integralmente ou pelo saldo que apresentar, no caso de rescisão por culpa do Contratado, sem prejuízo das penalidades cabíveis.
- 24.4.2. A garantia será restituída, automaticamente ou por solicitação, somente após integral cumprimento de todas as obrigações contratuais, inclusive recolhimento de multas e satisfação de prejuízos causados ao Contratante.
- 24.4.3. Em se tratando de modalidade fiança bancária, deverá constar do instrumento a expressa renúncia pelo fiador dos benefícios previstos nos arts. 827 e 835 do Código Civil.

25. DA PENALIDADE DE EXECUÇÃO

- 25.1. Conforme item 8 do Termo de Referência, anexo deste edital.
- 25.2. Conforme **cláusula décima terceira da Minuta do Contrato**, anexo deste edital.

26. DA RESCISÃO

- 26.1. Conforme **cláusula décima quarta da Minuta do Contrato**, anexo deste edital.

27. DA FISCALIZAÇÃO

- 27.1. Conforme item 9 do Termo de Referência, anexo deste edital.
- 27.2. Conforme **cláusula décima quinta da Minuta do Contrato**, anexo deste edital.

28. DAS PENALIDADES

- 28.1. No caso do fornecedor deixar de cumprir, total ou parcialmente, as obrigações assumidas no certame licitatório ou usar de má fé, ficará sujeita as penalidades abaixo discriminadas, assegurado seu direito ao contraditório e a ampla defesa.
- 28.2. **ADVERTÊNCIA**
28.2.1. Advertência pelo não cumprimento de obrigações assumidas, desde que não interfira na execução dos compromissos assumidos ou na sua conclusão e não traga sérios prejuízos econômicos e funcionais a este Órgão;
- 28.3. **MULTA**
28.3.1. De 0,25% ao dia, até o limite máximo de 5%, sobre o valor total **do Lote adjudicado**, nos casos de atraso injustificado nos prazos de **assinatura da ata de registro de preços**.
28.3.1.1. Após o 20º dia de atraso dos prazos previstos, sem justificativa aceita pela Administração, o objeto será considerado como inexecutado.
- 28.3.2. De 0,25% ao dia, até o limite máximo de 5%, sobre o valor total **do item solicitado**, nos casos de atraso injustificado nos prazos de **assinatura do Contrato; retirada/aceite da nota de empenho**.
28.3.2.1. Após o 20º dia de atraso dos prazos previstos, sem justificativa aceita pela Administração, o objeto será considerado como inexecutado.
- 28.3.3. De 0,25% ao dia, até o limite máximo de 5%, sobre o valor total **da respectiva nota de empenho**, nos casos de atraso injustificado nos prazos **entrega do objeto; substituição do objeto**.
28.3.3.1. Após o 20º dia de atraso dos prazos previstos, sem justificativa aceita pela Administração, o objeto será considerado como inexecutado.
- 28.3.4. De **10%**, sobre o valor total **do Lote adjudicado**, nos casos de recusa injustificada em assinar a **Ata de Registro de Preços**, se configurar inexecução total;
- 28.3.5. De **10%**, sobre o valor total **do item solicitado**, nos casos de:
I. Recusa injustificada em assinar o **Contrato**, se configurar inexecução total
II. Recusa injustificada em retirar/aceitar a **nota de empenho**, se configurar inexecução total;
- 28.3.6. De **10%**, sobre o valor total **da respectiva nota de empenho**, nos casos de:
I. Recusa injustificada em **entregar/executar o objeto**, se configurar inexecução total;
II. Recusa injustificada em substituir o objeto recusado ou com vícios, se configurar inexecução total;
III. Outras hipóteses de inexecução total do objeto.
- 28.3.7. De 10%, sobre o valor total **da respectiva nota de empenho**, nos casos de:
I. Recusa injustificada em retirar/aceitar a nota de empenho, se configurar inexecução parcial;
II. Entregar/executar parcial o objeto;
III. Recusa injustificada em substituir o objeto recusado ou com vícios, se configurar inexecução parcial;
IV. Outras hipóteses de inexecução parcial do objeto.
- 28.3.8. A inobservância do prazo fixado para apresentação da **garantia de execução do contrato** acarretará a aplicação de multa de 0,07% (sete centésimos por cento) do valor do contrato por dia de atraso, observado o máximo de 2% (dois por cento);

28.3.9. De 5% sobre o valor total **da respectiva nota de empenho** nos casos de irregularidade no cumprimento do objeto ou na prestação da garantia do produto do objeto contratado, não referidas nos itens anteriores

28.3.10. As multas são autônomas e a aplicação de uma não exclui a outra;

28.3.11. Havendo garantia à execução apresentada pela empresa, o valor da multa será descontado da mesma. Não havendo garantia ou caso o valor da multa seja superior à referida, a multa ou a diferença será cobrada administrativamente pela Contratante, podendo ser descontado dos créditos devidos, ou ainda judicialmente.

28.4. IMPEDIMENTO DE LICITAR

28.4.1. Ficará impedida de licitar e de contratar com o Estado do Pará e será descredenciada no SICAF/PA pelo prazo de até cinco anos, sem prejuízo das multas previstas no edital e no contrato, e das demais cominações legais, sendo-lhe assegurado o direito à ampla defesa, a licitante que, convocada dentro do prazo de validade de sua proposta:

- I. Não assinar o contrato;
- II. Deixar de entregar documentação exigida no edital;
- III. Apresentar documentação falsa;
- IV. Ensejar o retardamento da execução de seu objeto;
- V. Não manter a proposta;
- VI. Falhar ou fraudar na execução do contrato;
- VII. Comportar-se de modo inidôneo;
- VIII. Fizer declaração falsa ou cometer fraude fiscal.

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

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

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

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

28.9. As penalidades serão obrigatoriamente registradas no SICAF.

28.10. As sanções por atos praticados no decorrer da contratação estão previstas no Termo de Referência e na minuta do contrato.

29. DA FORMAÇÃO DO CADASTRO DE RESERVA

29.1. Após o encerramento da etapa competitiva, os licitantes poderão reduzir seus preços ao valor da proposta do licitante mais bem classificado.

29.2. A apresentação de novas propostas na forma deste item não prejudicará o resultado do certame em relação ao licitante melhor classificado.

29.3. Havendo um ou mais licitantes que aceitem cotar suas propostas em valor igual ao do licitante vencedor, estes serão classificados segundo a ordem da última proposta individual apresentada durante a fase competitiva.

29.4. Esta ordem de classificação dos licitantes registrados deverá ser respeitada nas contratações e somente será utilizada acaso o melhor colocado no certame não assine a ata ou tenha seu registro cancelado nas hipóteses previstas nos artigos 20 e 21 do Decreto nº 7.892/2013.

30. DA UTILIZAÇÃO DA ATA DE REGISTRO DE PREÇOS POR ÓRGÃO OU ENTIDADES NÃO PARTICIPANTES

30.1. Considerando a discricionariedade administrativa e diante da previsão expressa no artigo 24 do **Decreto Estadual 991, de 24 de agosto de 2020**, os órgãos não participantes poderão utilizar a ata de registro de preços decorrente deste certame, mediante a devida solicitação de adesão;

30.1.1. **Não poderão aderir os órgãos da administração pública federal**, nos termos do **Decreto Federal nº 7.892/2013**.

30.2. As adesões à Ata, se autorizadas pela Administração do Ministério Público, serão regidas pelo Artigo 22 do **Decreto Federal nº 7.892/2013**, e não poderão exceder, por órgão ou entidade, a **cinquenta** por cento dos quantitativos dos itens do instrumento convocatório e registrados na Ata de Registro de Preços para o órgão gerenciador;

30.2.1. O deferimento de adesão será submetido à avaliação de sua conveniência e ausência de prejuízo para as demandas do Ministério Público, devendo observar as condições do art. 22, § 1º-A e a publicação referida no § 1º-B, do mesmo decreto, além de outras previsões daquela norma:

"Art. 22. [...].

§ 1º-A A manifestação do órgão gerenciador de que trata o § 1º fica condicionada à realização de estudo, pelos órgãos e pelas entidades que não participaram do registro de preços, que demonstre o ganho de eficiência, a viabilidade e a economicidade para a administração pública federal da utilização da ata de registro de preços, conforme estabelecido em ato do Secretário de Gestão do Ministério do Planejamento, Desenvolvimento e Gestão. (Incluído pelo Decreto nº 9.488, de 2018)

§ 1º-B O estudo de que trata o § 1º-A, após aprovação pelo órgão gerenciador, será divulgado no Portal de Compras do Governo federal. (Incluído pelo Decreto nº 9.488, de 2018)"

30.2.2..

30.3. 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 para o órgão gerenciador, independentemente do número de órgãos não participantes que aderirem, conforme abaixo:

Item	Quantidade Registrada	Adesão por cada órgão não participante	Adesão considerando todos os órgãos não participantes
01	134	67	268
02	20	10	40
03	02	1	04
04	01	0	0
05	01	0	0
06	20	10	40

30.4. As demais regras referentes aos órgãos gerenciador e participantes, bem como a eventuais adesões são as que constam da minuta de Ata de Registro de Preços.

31. DA REVOGAÇÃO E DA ANULAÇÃO

31.1. A autoridade competente para homologar o procedimento licitatório de que trata este Decreto poderá revogá-lo somente em razão do interesse público, por motivo de fato superveniente devidamente comprovado, pertinente e suficiente para justificar a revogação, e deverá anulá-lo por ilegalidade, de ofício ou por provocação de qualquer pessoa, por meio de ato escrito e fundamentado (art. 50, Decreto Federal nº 10.024/2019).

31.1.1. Os licitantes não terão direito à indenização em decorrência da anulação do procedimento licitatório, ressalvado o direito do contratado de boa-fé ao ressarcimento dos encargos que tiver suportado no cumprimento do contrato.

32. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

- 32.1. Até **02 (dois) dias úteis** antes da data fixada para abertura da sessão pública, qualquer pessoa poderá impugnar o ato convocatório do pregão, na forma eletrônica (**art. 24, Decreto Estadual nº 534/2020**).
- 32.1.1. A impugnação deverá ser encaminhada exclusivamente por meio eletrônico, no e-mail pregao@mppa.mp.br, não sendo aceitas pela administração outras formas de envio;
- 32.1.2. Caberá ao Pregoeiro, auxiliado pelos responsáveis pela elaboração deste Edital e seus anexos, decidir sobre a impugnação no prazo de **24 (vinte e quatro) horas**, contado da data de recebimento da impugnação.
- 32.1.3. Acolhida a impugnação, será definida e publicada nova data para a realização do certame.
- 32.2. Os pedidos de esclarecimentos referentes a este processo licitatório deverão ser enviados ao Pregoeiro, até 03 (três) dias úteis anteriores à data designada para abertura da sessão pública, exclusivamente por meio eletrônico via internet, no e-mail pregao@mppa.mp.br, não sendo aceitas pela administração outras formas de envio.
- 32.2.1. O Pregoeiro responderá aos pedidos de esclarecimentos no prazo de 2 (dois) dias úteis, contado da data de recebimento do pedido, e poderá requisitar subsídios formais aos responsáveis pela elaboração do Edital e dos anexos.
- 32.3. As impugnações e pedidos de esclarecimentos não suspendem os prazos previstos no certame.
- 32.3.1. A concessão de efeito suspensivo à impugnação é medida excepcional e deverá ser motivada pelo pregoeiro, nos autos do processo de licitação.
- 32.4. As respostas aos pedidos de esclarecimentos serão divulgadas pelo sistema e vincularão os participantes e a Administração.

33. DAS DISPOSIÇÕES GERAIS

- 33.1. Da sessão pública do Pregão divulgar-se-á Ata no sistema eletrônico.
- 33.2. Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário anteriormente estabelecido, desde que não haja comunicação em contrário, pelo Pregoeiro.
- 33.3. Todas as referências de tempo no Edital, no aviso e durante a sessão pública observarão o horário de Brasília – DF.
- 33.4. No julgamento das propostas e da habilitação, o Pregoeiro poderá sanar erros ou falhas que não alterem a substância das propostas, dos documentos e sua validade jurídica, mediante despacho fundamentado, registrado em ata e acessível a todos, atribuindo-lhes validade e eficácia para fins de habilitação e classificação.
- 33.5. A homologação do resultado desta licitação não implicará direito à contratação.
- 33.6. As normas disciplinadoras da licitação serão sempre interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse da Administração, o princípio da isonomia, a finalidade e a segurança da contratação.
- 33.7. Os licitantes assumem todos os custos de preparação e apresentação de suas propostas e a Administração não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório.
- 33.8. Na contagem dos prazos estabelecidos neste Edital e seus Anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento. Só se iniciam e vencem os prazos em dias de expediente na Administração.
- 33.9. O desatendimento de exigências formais não essenciais não importará o afastamento do licitante, desde que seja possível o aproveitamento do ato, observados os princípios da isonomia e do interesse público.
- 33.10. Em caso de divergência entre disposições deste Edital e de seus anexos ou demais peças que compõem o processo, prevalecerá as deste Edital.
- 33.11. O Edital está disponibilizado, na íntegra, nos endereços eletrônicos www.mppa.mp.br e www.comprasgovernamentais.gov.br, e também poderão ser lidos e/ou obtidos no

endereço Rua João Diogo, 100, 4º Andar, Cidade Velha, Belém-Pará, CEP 66015-165, nos dias úteis, no horário das 08:00 horas às 17:00 horas, nas sextas-feiras até as 14:00 horas, mesmo endereço e período no qual os autos do processo administrativo permanecerão com vista franqueada aos interessados.

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

- 33.12.1. ANEXO I - Termo de Referência
- 33.12.2. ANEXO II – Minuta de Ata de Registro de Preços
- 33.12.3. ANEXO III – Minuta de Termo de Contrato
- 33.12.4. ANEXO IV – Modelo de Declaração de Cumprimento da Resolução nº 037/2009-CNMP (vedação às práticas de nepotismo)

Belém (Pa), 22 de fevereiro de 2021

GILBERTO VALENTE MARTINS
Procurador-Geral de Justiça

ANEXO I

TERMO DE REFERÊNCIA

1 OBJETO

- 1.1. A presente licitação tem por objeto o **Registro de Preços para aquisição de ativos de segurança de rede, Firewalls Next Generation (NGFW) com SD-WAN integrada, contemplando os serviços de Instalação, Treinamento e Suporte Técnico.**

2 JUSTIFICATIVA DA CONTRATAÇÃO

2.1. A rede de computadores do Ministério Público do Estado do Pará (MPPA) abrange o prédio Sede, onde encontra-se o Datacenter, mais sete prédios no seu em torno, compondo o campus da Cidade Velha. Mas há também as unidades remotas, ou seja, fora da sede, em Belém e diversas promotorias nas cidades do Estado do Pará. Nestas unidades remotas não há equipamento de firewall adequado, que provenha proteção de perímetro e borda da rede de computadores, interconexão segura com a Sede via *Virtual Private Network* (VPN), que permita bloquear, filtrar, priorizar e redirecionar trafico da rede, ou seja, que possibilite implementar políticas de segurança, de utilização da rede, de controle de aplicações e acesso à internet.

2.2. Dentre as diversas finalidades para a aquisição de *Firewalls Next Generation* (NGFW) com SD-WAN, destaca-se:

2.3. Primeiramente, considerando a Resolução nº 06/95 do Colégio de Procuradores de Justiça, que em seu capítulo II, artigo 11º, I, estabelece as competências do Departamento de Informática, dentre elas a de planejar, coordenar, e orientar as atividades de informática e banco de dados do Ministério Público, faz-se necessário a aquisição de bens permanente que permitam aos Membros desta Instituição o cumprimento de suas atribuições.

2.4. Segundo, o NGFW deve auxiliar na segurança da informação, figurando como a primeira camada de proteção da rede de computadores das unidades remotas, a fim de prover proteção de perímetro e borda da rede de computadores das Promotorias de Justiça e unidades fora da sede deste *Parquet*, haja vista, atualmente não existir firewall nestas unidades.

2.5. A terceira finalidade, visa fornecer condições seguras de acesso a sistemas sensíveis da instituição, que não podem ser disponibilizados diretamente na internet sob o risco de vazamento de informações sob sigilo, através de *Virtual Private Network* (Rede Virtual Privada), permitir, bloquear, filtrar, redirecionar, controlar o acesso a aplicações internas e externas, sites internos e Internet. Além de assegurar e controlar o acesso à rede de computadores das unidades remotas deste Ministério Público.

2.6. A quarta finalidade decorre da necessidade de otimizar a utilização dos links de dados das unidades remotas, permitir failover, balanceamento de carga, escolha dinâmica do melhor caminho de roteamento, conforme regras de negócio e de aplicações na camada de aplicação por meio da funcionalidade de SD-WAN.

2.7. A quinta finalidade é facilitar e agilizar a implantação de VPN segura, sem necessidade de configuração nas unidades remotas, garantir a continuidade da conexão da VPN entre as promotorias de justiça e a sede em casos de falhas em um dos links de dados, assegurando também o acesso à Internet.

2.8. Como sexta finalidade, necessidade de suportar à crescente demanda por conectividade de rede, internet e acesso a sistemas internos como o SIMP, GEDOC, Webmail, SIAMP, PJE dentre outros:

2.8.1. Ao aumento de novos serviços online prestados pelo Ministério (sistemas, correio eletrônico, acesso à Internet, Ponto online);

2.8.2. A expansão das áreas físicas e instalações prediais;

2.8.3. A necessidade de adequar novas soluções de tecnologia da informação previamente adquiridas e comportar novas soluções de tecnologia da informação a serem adquiridas;

2.8.4. Ao aumento no número de usuários e prestação de serviços a estes que deve ocorrer de maneira rápida, segura e eficaz.

2.9. A sétima finalidade, é atender a crescente dependência dos recursos de tecnologia da informação, que fazem com que a infraestrutura de rede deva apresentar cada vez maior confiabilidade, resiliência, disponibilidade, segurança, capacidade de resolução de problemas de maneira proativa e rápida e melhorar a experiência para todos os usuários da rede do Ministério Público do Estado do Pará.

2.10. A oitava finalidade é de permitir uma gestão centralizada de todos dos dispositivos de segurança e borda da rede das unidades remotas, otimizando o monitoramento do uso da rede local nas promotorias de justiça e unidades fora da sede, agilizar também a recuperação de desastres (disaster recovery).

2.11. Por último, a ampliação da infraestrutura de rede existente nos Polos do Ministério Público do Pará, torna necessário assegurar uma maior estabilidade da rede e dos sistemas por ela suportados tendo em vista a criticidade dos mesmos e necessidade de garantir o funcionamento ininterrupto e seguro do ambiente de rede.

2.12. Esta solução visa implantar equipamentos que viabilizam a conectividade segura entre as redes locais das promotorias de justiça do interior do Estado com o prédio Sede (Datacenter) e Internet. A Solução deve concentrar em um único equipamento novo, do tipo appliance, as funcionalidades de firewall de próxima geração (NGFW) e SD-WAN com gerenciamento centralizado.

2.13. Quanto à funcionalidade de NGFW a solução dentre outras coisas deve propiciar segurança de informação perimetral que inclui filtro de pacote, controle de aplicação na camada 7 (camada de aplicação), administração de largura de banda (QoS), VPN, IPSec e SSL, IPS, prevenção contra ameaças de vírus, spywares e malwares “Zero Day”, Filtro de URL, Possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos de firewall, permitir controle global de políticas para todos os equipamentos que compõe a plataforma de segurança, compatibilidade para estabelecer VPN segura com o firewall existente no Datacenter (PA3020).

2.14. A funcionalidade de SD-WAN vai otimizar implantações de links de dados e VPN nas promotorias de justiça, automatizar o caminho das WANs, possibilitar automação do controle do caminho baseado em políticas de negócios e aplicações; definição dinâmica de caminhos e métricas, baseadas na visibilidade em tempo real, sobre o destino desejado da aplicação, seu desempenho, a experiência do usuário final da aplicação e a qualidade das redes disponíveis no caminho; automação alinhada aos negócios e baseada em políticas para definir a qualidade do serviço e privilégios de acesso para todas as aplicações e todos os usuários, em combinação com a escolha automatizada do caminho; monitoramento de desempenho integrado de ponta a ponta e otimização da WAN de forma segura. Gerenciamento centralizado, com uma visualização integrada e topologia “full mesh” da estrutura de conectividade entre o datacenter e filiais; tudo em uma plataforma de gerenciamento integrada e centralizada, que possibilite automatizar a implantação da VPN, com escolha do melhor link de dados e melhor caminho para a VPN, possibilitar múltiplas VPN's e continuidade do serviço de VPN em caso de falhas ou degradação de um dos links de dados, melhorando a conectividade entre redes das filiais e a sede; que possibilite aplicar regras de controle de acesso, desempenho e segurança com base na política definida no console de gerenciamento central; com suporte a VLANs, capacidade de segregar tráfego pelas WANs e entre redes LANs sem fio, e com fio na filial; capacidade de segregar tráfego com base nas aplicações da camada 7; a implantação deve ser sem configurações na unidade remota “zero-touch” via ativação automatizada e segura de todos os gateways de WAN.

2.15. Desta forma, pelo exposto acima, ressalta-se a necessidade de aquisição de Firewalls do tipo NGFW, com SD-WAN integrada para todas as unidades remotas (Polos, Promotorias de Justiça). Esses dispositivos de rede são imprescindíveis para aumentar a segurança na rede destas unidades, bem como, possibilitar otimização da WAN e conexão segura com a sede, atuar como primeiro nível de segurança, possibilitar restringir os riscos e minimizar os impactos nos sistemas e na rede deste Parquet.

2.16. A aquisição através de Ata de Registro de Preços se faz necessária, em razão da imprevisibilidade na aquisição da demanda, pois os referidos equipamentos serão utilizados para: implementar o serviço de rede em prédios da Instituição que a ainda não contam com o tal; substituição de equipamentos danificados e fora do prazo de garantia; e substituição de equipamentos danificados com dano não cobertos pela garantia. Considerando, por fim, que não há nenhum planejamento institucional quanto à alteração no número de Promotorias, de prédios e de pessoas, verifica-se que é impossível determinar, dentro do número máximo de unidades do MP/PA, quantos equipamentos serão necessários no decorrer do período de validade da Ata de Registro de Preços.

2.17. Ademais, a contratação através da Ata de Registro de Preços garante também ao MP/PA que não serão adquiridos equipamentos além dos necessários para suprir a demanda existente e aquela que vier a ocorrer, aliado ao fato de que a Instituição não possui espaço específico para armazenagem de longo prazo para esse tipo de equipamento.

2.18. Há de se considerar também que o prazo de garantia dos equipamentos é contado a partir da sua entrega e, como o Ministério público não dispõe de equipe técnica e infraestrutura necessária para a implantação de todos os equipamentos ao mesmo tempo, entendemos que poderíamos estar causando

danos à Instituição ao perder prazo de garantia de equipamentos estocados, reduzindo-se custos de armazenamento e otimização de prazo de garantia. O caso em tela enquadra-se nas hipóteses previstas no Art. 4º, I e IV do Decreto Estadual 876/2013”.

3 ESPECIFICAÇÕES DOS BENS

CLASSIFICAÇÃO GLOBAL POR LOTE

LOTE ÚNICO						
Item	CODBB CATMAT	Descrição	Und	Qtd	Preço Máximo Unitário	Preço Estimado do Item
1	150100	NGFW de pequeno porte com SD-WAN integrada, garantia, suporte e todas as licenças necessárias para atender a demanda do MPPA	Und	134	36.650,17	4.911.122,78
2	150100	NGFW de médio porte com SD-WAN integrada, garantia, suporte e todas as licenças necessárias para atender a demanda do MPPA	Und	20	140.185,00	2.803.700,00
3	70653	Concentrador de VPN com SD-WAN integrada, garantia, suporte e todas as licenças necessárias para atender a demanda do MPPA	Und	02	365.336,67	730.673,34
4	27472	Sistema de Gerência Centralizada para, no mínimo, 160 dispositivos (Pontos de Presença)	Und	01	169.024,00	169.024,00
5	26972	Serviço de Instalação/Configuração	Und	01	137.333,33	137.333,33
6	20052	Treinamento “Hands On” sobre Solução de Firewall/SD-WAN	Horas	20h	1.020,00	20.400,00
Valor Total do Lote Único						8.772.253,45

Obs.: Em relação aos itens de 1 a 4, a proposta deverá conter a lista de **PART NUMBERS** do fabricante e suas respectivas quantidades necessárias para atender as características técnicas solicitadas neste edital;

Obs.: A proposta apresentada em desacordo com este edital será desclassificada;

Obs.: A aquisição será feita em 1 (um) único lote referente aos itens firewalls de pequeno porte, firewalls de médio porte, concentrador de VPN, sistema de gerência centralizada, serviço de instalação/configuração e treinamento. A aquisição pretendida requer a total compatibilidade entre os equipamentos ofertados nos itens 01 a 03, sendo possível somente se estes forem do mesmo fabricante. Além disso, devem ser fornecidos acessórios para configuração e instalação dos equipamentos (como cabo console, abas de fixação, parafusos), os acessórios devem ser integralmente compatíveis com os itens 01 a 03, quando indispensáveis para a utilização e configuração dos equipamentos. Assim, torna-se necessário consolidar esses itens em um único grupo (lote), para garantir que os equipamentos sejam do mesmo fabricante, sejam compatíveis entre si, preservando a interoperabilidade entre eles e possibilitando gerência centralizada. Além disso, visa-se garantir a padronização na instalação e configuração dos mesmos, de acordo com as necessidades deste Parquet, bem como assegurar que o treinamento do tipo “Hands On” seja único e com base nos requisitos do caso concreto do MPPA. Vale ressaltar ainda que, devido ao número limitado de servidores, é mais eficiente e econômico gerenciar e fiscalizar um único contrato e gerir o suporte técnico com uma única CONTRATADA.

Obs.: Todo o lote deve ser fornecido por um único fornecedor, não sendo possível fornecer apenas alguns itens deste lote. A oferta deve cobrir todos os itens do lote.

Obs.: O código do **COMPRASNET** informado no campo especificação é genérico e em caso de divergência entre a descrição e/ou descrição detalhada do item cadastrada no *comprasgovernamentais* e as consignadas no termo de referência, prevalecem as consignadas no termo de referência.

Obs.: Não serão aceitas propostas com especificações diferentes e quantidades inferiores às estimadas em cada item, nem com falta de itens nos lotes.

Obs.: Os valores deverão ser calculados com duas casas decimais.

ESPECIFICAÇÃO DETALHADA DOS EQUIPAMENTOS E LICENÇAS

3.1. DESCRIÇÃO

3.1.1. Aquisição de solução de proteção de rede com características de Firewall Next Generation (NGFW) com SD-WAN integrada do tipo Appliance. A solução deve ser integralmente do mesmo fabricante, contemplando gerência centralizada, todos os softwares e suas licenças de uso, possibilitando atualização contínua. Deve incluir, além das funcionalidades citadas acima: Otimização de WAN, gerenciamento centralizada, zero-touch deployment, filtro de pacote, controle de aplicação, administração de largura de banda (QoS), VPN, IPSec e SSL, IPS, prevenção contra ameaças de vírus, spywares e malwares “Zero Day”, Filtro de URL, bem como controle de transmissão de dados e acesso à internet compondo uma plataforma de segurança integrada e robusta. Na qual todos os links WANs e VPNs devem funcionar simultaneamente;

3.1.2. Por plataforma de segurança entende-se hardware e software integrados do tipo appliance com todas as licenças necessárias inclusas, o sistema operacional fornecido deve ser a versão mais nova disponível, devendo, entretanto, ser considerada estável pelo fabricante do equipamento;

3.1.3. A solução de NGFW deverá suportar mecanismos de redundância de dispositivos em modo ativo-passivo e ativo-ativo, em caso de falha de um dos equipamentos;

3.1.4. Deve possuir LEDs indicadores de status, atividade de rede, status dos links e alimentação;

3.1.5. O equipamento ofertado deve ser compatível com as seguintes funcionalidades:

3.1.5.1. Possibilitar a coleta de estatísticas de todo o tráfego que passar pelo firewall;

3.1.5.2. A solução deve apresentar informações de relatório de acordo com um intervalo de tempo definido pelo administrador;

3.1.5.3. A solução deve contemplar gerenciamento centralizado e integrado de todos os dispositivos da sede e filiais, que possibilite que as configurações, controle de acesso, regras e políticas sejam executadas em um único ponto e replicadas para todos os dispositivos, grupos de dispositivos, usuários, grupos de usuários;

3.1.5.4. O equipamento deve permitir a gestão e monitoramento através da interface de gestão WEB no mesmo dispositivo de proteção da rede;

3.1.5.5. Permitir controle global e centralizado de políticas para todos os equipamentos que compõe a plataforma de segurança;

3.1.5.6. Exportar backup de configuração automaticamente via agendamento;

3.1.5.7. Os hardwares e softwares ofertados na composição deste item não devem estar listados como “end-of-sale”, “end-of-support” ou “end-of-life” por seus respectivos fabricantes na data da abertura das propostas. Não serão aceitos equipamentos que entrem em modo End of Support durante a vigência da garantia ou que entre em modo End of Life pelo período de 1 ano após a assinatura do contrato.

3.2. SD-WAN

3.2.1. Deve possuir capacidade para utilizar, pelo menos 3 (três) links de WAN, sendo no mínimo 2 (dois) links simultâneos.

3.2.2. Realizar balanceamento de tráfego de saída entre os links de Wan primários;

3.2.3. Permitir que a escolha do link WAN de saída seja influenciada por regras definidas pelo administrador de rede da CONTRATANTE e dinamicamente. As regras devem permitir ao menos um dos parâmetros a seguir ou combinação destes:

3.2.4. Endereço IP de origem e/ou destino;

3.2.5. Subredes de origem e/ou destino;

3.2.6. Métricas de Jitter, latência e perda de pacotes por aplicação;

3.2.7. Status da porta de WAN primários (UP ou DOWN);

3.2.8. Toda a comunicação Wan deve trafegar em um túnel VPN ponto-a-ponto estabelecido dinamicamente entre os PONTOS DE PRESENÇA da CONTRATANTE;

3.2.9. Suportar o protocolo de tunelamento GRE (General Routing Encapsulation - RFC 2784);

3.2.10. A solução deve ter um tempo máximo de failover e failback de 300 segundos;

3.2.11. A topologia da rede WAN deve ser dentre outras possíveis, a de malha completa (full mesh);

3.2.12. O estabelecimento do túnel VPN entre os PONTOS DE PRESENÇA pode inicialmente ser orientado pelo concentrador, mas o tráfego de dados após o estabelecimento do túnel deve ser realizado diretamente entre os integrantes do túnel, sem consumir throughput do concentrador;

3.2.13. A solução de SD-WAN deverá ser integrada no próprio appliance de NGFW, não sendo aceito quaisquer componentes adicionais com esta função.

CARACTERÍSTICAS GERAIS

3.3. Por cada equipamento que compõe a plataforma de segurança, entende-se o hardware e as licenças de softwares necessárias para o seu funcionamento;

3.4. Na data da proposta, nenhum dos modelos ofertados poderão estar listados como “*end-of-sale*”, “*end-of-support*” ou “*end-of-life*” por seus respectivos fabricantes. Não serão aceitos equipamentos que entrem em modo *End of Support* durante a vigência da garantia ou que entre em modo *End of Life* pelo período de 1 ano após a assinatura do contrato;

3.5. A solução deve consistir do *appliance* de proteção de rede com funcionalidades de *Next Generation Firewall* (NGFW) e SD-WAN, além de Solução de Gerência Centralizada com Sistema de Armazenamento de Log e Relatórios Centralizados;

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

3.7. As funcionalidades de proteção de rede (Firewall, IPS, Antivírus, Filtro Web, Controle de aplicações) que compõem a plataforma de segurança, devem funcionar localmente nos dispositivos NGFW;

3.8. A funcionalidade de *Sandbox* deve ser executada em nuvem pelo próprio fabricante, devendo o NGFW estar devidamente licenciado para possibilitar a execução desta função;

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

3.10. O hardware e software que executa as funcionalidades de proteção de rede firewall (NGFW) e SD-WAN deve ser do tipo *appliance*. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

3.11. Os *appliances* que executarão a função de NGFW deverão ter altura máxima de 1 (um) U de espaço em rack;

3.12. O software deverá ser fornecido em sua versão mais atualizada e estável;

3.13. Os equipamentos deverão ser fornecidos de acordo com as características técnicas mínimas presentes neste Termo de Referência;

3.14. A solução deverá ser capaz de fechar túneis VPN do tipo IPSec com equipamentos de terceiros (Palo Alto Networks, Cisco, Check Point, Juniper, Fortinet, SonicWall);

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

3.15.1. Suporte a 4094 VLAN Tags 802.1q;

3.15.2. Agregação de links 802.3ad e LACP;

3.15.3. Policy based routing ou policy based forwarding;

3.15.4. Roteamento multicast (PIM-SM e PIM-DM);

3.15.5. DHCP Relay;

3.15.6. DHCP Server;

3.15.7. Jumbo Frames;

3.16. Os dispositivos de proteção de rede devem suportar *sFlow*;

3.17. Suportar sub-interfaces ethernet logicas.

3.18. Deve suportar os seguintes tipos de NAT:

3.18.1. Nat dinâmico (Many-to-1);

3.18.2. Nat dinâmico (Many-to-Many);

3.18.3. Nat estático (1-to-1);

3.18.4. NAT estático (Many-to-Many);

3.18.5. Nat estático bidirecional 1-to-1;

3.18.6. Tradução de porta (PAT);

3.18.7. NAT de Origem;

3.18.8. NAT de Destino;

3.18.9. Suportar NAT de Origem e NAT de Destino simultaneamente.

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

3.18.11. Deve implementar o protocolo ECMP;

- 3.18.12. Portas UDP, uma ou um range;
- 3.18.13. Portas TCP, uma ou um range;
- 3.18.14. Deve implementar balanceamento de link por hash do IP de origem;
- 3.18.15. Deve implementar balanceamento de link por hash do IP de origem e destino;
- 3.18.16. Deve implementar balanceamento de link através do método round-robin;
- 3.18.17. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, três links;
- 3.18.18. Deve implementar balanceamento de link através de políticas por usuário e grupos de usuários do LDAP/AD;
- 3.18.19. Seleção do melhor caminho que o tráfego da sessão leva com base na qualidade do circuito baseado em Latência, Perda "Loss" e Jitter;
- 3.18.20. A solução deve ser capaz de detectar perda, aumento de latência e jitter de um caminho, quando este começa a degradar a qualidade de uma aplicação. Deslocando o tráfego da aplicação para outro circuito de modo que esteja com melhor desempenho de forma transparente para os usuários, sem que seja percebido interrupção na continuidade do aplicativo ou dos pacotes perdidos;
- 3.18.21. Deve implementar balanceamento de link através de políticas por aplicação, conforme regras de negócio;
- 3.18.22. Deve implementar o protocolo Link Layer Discovery (LLDP), permitindo que o appliance e outros ativos da rede se comuniquem para identificação da topologia da rede em que estão conectados e a função dos mesmos facilitando o processo de troubleshooting. As informações aprendidas e armazenadas pelo appliance devem ser acessíveis via SNMP;
- 3.18.23. Enviar log para sistemas de monitoração externos, simultaneamente;
- 3.18.24. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;
- 3.18.25. Deve permitir configurar certificado caso necessário para autenticação no sistema de monitoração externo de logs;
- 3.18.26. Proteção contra anti-spoofing;
- 3.18.27. Deve permitir bloquear sessões TCP que usem variações do 3-way hand-shake, como 4 way e 5 way split hand-shake, prevenindo desta forma possíveis tráfegos maliciosos;
- 3.18.28. Deve exibir nos logs de tráfego o motivo para o término da sessão no firewall, incluindo sessões finalizadas onde houver de-criptografia de SSL e SSH;
- 3.18.29. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
- 3.18.30. Para IPv6, deve suportar roteamento estático e dinâmico (RIPv6, BGP4+, OSPFv3);
- 3.18.31. Suportar a OSPF graceful restart;
- 3.18.32. Suportar no mínimo as seguintes funcionalidades em IPv6: SLAAC (address auto configuration), NAT64, Identificação de usuários a partir do LDAP/AD, IPv6 over IPv4 IPSec, Regras de proteção contra DoS (Denial of Service), De-criptografia SSL e SSH, PBF (Policy Based Forwarding), QoS, DHCPv6 Relay, DHCPv6 Server, IPSec, Ativo/Ativo, Ativo/Passivo, SNMP, NTP, SYSLOG, DNS e controle de aplicação;
- 3.18.33. Dispositivos de proteção devem ter a capacidade de operar de forma simultânea em uma única instância de firewall, mediante o uso de suas interfaces físicas nos seguintes modos: Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);
- 3.18.34. Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
- 3.18.35. Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
- 3.18.36. Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;
- 3.18.37. Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
- 3.18.38. Suporte à configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;
- 3.18.39. Em modo transparente;
- 3.18.40. Em Layer 3;
- 3.18.41. A configuração em alta disponibilidade deve sincronizar;
- 3.18.42. Sessões;
- 3.18.43. Configurações, incluindo, mas não limitado a políticas de Firewall, NAT, QOS e objetos de rede;
- 3.18.44. Certificados de-criptografados;

3.18.45.Associações de Segurança das VPNs;

3.18.46.Sincronizar tabelas FIB;

3.18.47.HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link;

O gerenciamento da solução deve suportar acesso via SSH e interface WEB (HTTPS), incluindo, mas não limitado à, exportar configuração dos sistemas virtuais (contextos) por ambas interfaces;

3.18.48.As funcionalidades de NGFW e SD-WAN, controle de aplicações, VPN IPsec e SSL, QOS, SSL e SSH Decryption e protocolos de roteamento dinâmico devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante.

3.19. CONTROLE POR POLÍTICA DE FIREWALL

3.19.1. Deverá suportar controles por zona de segurança;

3.19.2. O Firewall deverá possuir controles de segurança de camada L4 - L7;

3.19.3. A solução de firewall deve atuar na camada de aplicação possibilitando ao administrador criar regras e impedir a utilização de aplicações (*deep packet inspection*);

3.19.4. Controles de políticas por porta e protocolo;

3.19.5. Controle de políticas por aplicações grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;

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

3.19.7. Deve suportar a consulta a fontes externas de endereços IP, domínios e URLs podendo ser adicionados nas políticas de firewall para bloqueio ou permissão do tráfego;

3.19.8. Controle de políticas por código de País ou geolocalização (Por exemplo: BR, USA, UK, RUS);

3.19.9. Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (*Inbound*) e Saída (*Outbound*).

3.19.10.Deve suportar *offload* de certificado em inspeção de conexões SSL de entrada (*Inbound*);

3.19.11.Deve de-criptografar tráfego *Inbound* e *Outbound* em conexões negociadas com TLS 1.2;

3.19.12.Controle de inspeção e de-criptografia de SSH por política;

3.19.13.A de-criptografia de SSH deve possibilitar a identificação e bloqueio de tráfego caso o protocolo esteja sendo usado para tunelar aplicações como técnica evasiva para burlar os controles de segurança;

3.19.14.A plataforma de segurança deve implementar espelhamento de tráfego de-criptografado (SSL e TLS) para soluções externas de análise (Forense de rede, DLP, Análise de Ameaças, entre outras);

3.19.15.Bloqueios dos seguintes tipos de arquivos: bat, cab, dll, exe, pif e reg;

3.19.16.*Traffic shaping* QoS baseado em Políticas (Prioridade, Garantia e Máximo);

3.19.17.QoS baseado em políticas para marcação de pacotes (*diffserv marking*), inclusive por aplicações;

3.19.18.Suporte a objetos e regras IPV6;

3.19.19.Suporte a objetos e regras *multicast*;

3.19.20.Deve possibilitar a utilização de no mínimo 04 ações nas regras de controle como Permitir, Bloquear;

3.19.21.Deve suportar no mínimo os seguintes tipos de negação de tráfego nas políticas de firewall: *Drop* sem notificação do bloqueio ao usuário e TCP-Reset para o cliente;

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

3.19.23.O controle por políticas de firewall deverá ser integrado no próprio *appliance* de NGFW, não sendo aceito quaisquer componentes adicionais com esta função.

3.20. CONTROLE DE APLICAÇÕES

3.20.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;

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

3.20.3. Reconhecer pelo menos 2000 (duas mil) aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a *peer-to-peer*, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

3.20.4. Reconhecer pelo menos as seguintes aplicações: *bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, onedrive, db2, mysql, oracle, active directory,*

kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs, etc;

3.20.5. Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações customizadas e não somente sobre aplicações conhecidas;

3.20.6. Deve inspecionar o *payload* de pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo. A checagem de assinaturas também deve determinar se uma aplicação está utilizando a porta default ou não, incluindo, mas não limitado a RDP na porta 80 ao invés de 389;

3.20.7. Deve aplicar heurística a fim de detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a *Encrypted Bittorrent* e aplicações VOIP que utilizam criptografia proprietária;

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

3.20.9. 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, incluindo, mas não limitado a Yahoo *Instant Messenger* usando HTTP. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do Webex. Além de detectar arquivos e outros conteúdos que devem ser inspecionados de acordo as regras de segurança implementadas;

3.20.10. Deve permitir a utilização de aplicativos para um determinado grupo de usuário e bloquear para o restante, incluindo, mas não limitado a Skype. Deve permitir também a criação de políticas de exceção concedendo o acesso a aplicativos como Skype apenas para alguns usuários;

3.20.11. Identificar o uso de táticas evasivas via comunicações criptografadas;

3.20.12. Atualizar a base de assinaturas de aplicações automaticamente;

3.20.13. Reconhecer aplicações em IPv6;

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

3.20.15. 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 *Domain Controller*, nem nas estações dos usuários;

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

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

3.20.18. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão;

3.20.19. A criação de assinaturas personalizadas deve permitir o uso de expressões regulares, contexto (sessões ou transações), usando posição no *payload* dos pacotes TCP e UDP e usando decoders de pelo menos os seguintes protocolos: HTTP, FTP, SMTP, Telnet, SSH, MS-SQL, IMAP, MS-RPC e RTSP.

3.20.20. Deve alertar o usuário quando uma aplicação for bloqueada;

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

3.20.22. Deve possibilitar a diferenciação de tráfegos Peer2Peer (*Bittorrent*, emule, etc.) possuindo granularidade de controle/políticas para os mesmos;

3.20.23. Deve possibilitar a diferenciação de tráfegos para as seguintes aplicações e respectivas granularidades: Instagram (login, post, vídeo, upload de arquivo), YouTube (canais, streaming HD, pesquisa de vídeo, play vídeo), Facebook (upload e download de arquivos, login, chat, botão de like, chamadas VoIP, play vídeo, post, mensagem de voz), WhatsApp (transferência de arquivos, chamadas VoIP e whatsapp web);

3.20.24. Deve possibilitar a diferenciação de aplicações Proxies, possuindo granularidade de controle/políticas para os mesmos;

3.20.25. Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como: Tecnologia utilizada nas aplicações (Client-Server, Browser Based, Network Protocol, etc); Nível de risco da aplicação; Categoria de aplicações;

3.20.26. Deve ser possível configurar *Application Override* permitindo selecionar aplicações individualmente;

3.20.27. Aplicações que usem técnicas evasivas, utilizadas por *malwares*, como transferência de arquivos e/ou uso excessivo de banda, etc.

3.20.28. O controle de aplicações deverá ser integrado no próprio *appliance* de NGFW, não sendo aceito quaisquer componentes adicionais com esta função.

3.21. PREVENÇÃO DE AMEAÇAS

3.21.1. Para proteção do ambiente de redes contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio *appliance* de Firewall;

3.21.2. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);

3.21.3. As funcionalidades de IPS, Antivírus e *Anti-Spyware* devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;

3.21.4. Deve sincronizar as assinaturas de IPS, Antivírus, *Anti-Spyware* quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;

3.21.5. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS, *Anti-Spyware* e Antivírus: permitir, permitir e gerar log, bloquear, e enviar tcp-reset;

3.21.6. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;

3.21.7. Deve suportar granularidade nas políticas de IPS Antivírus e *Anti-Spyware*, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

3.21.8. Deve permitir o bloqueio de vulnerabilidades;

3.21.9. Deve permitir o bloqueio de *exploits* conhecidos;

3.21.10. Deve incluir proteção contra ataques de negação de serviços;

3.21.11. Fornecem proteção contra ataques de dia zero;

3.21.12. Deverá possuir os seguintes mecanismos de inspeção de IPS:

3.21.13. Análise de padrões de estado de conexões;

3.21.14. Análise de decodificação de protocolo;

3.21.15. Análise para detecção de anomalias de protocolo;

3.21.16. Análise heurística;

3.21.17. IP *Defragmentation*;

3.21.18. Remontagem de pacotes de TCP.

3.21.19. Bloqueio de pacotes malformados.

3.21.20. Ser imune e capaz de impedir ataques básicos como: Synflood, ICMPflood, UDPflood, etc;

3.21.21. Detectar e bloquear a origem de portscans;

3.21.22. Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;

3.21.23. Suportar os seguintes mecanismos de inspeção contra ameaças de rede: análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, análise heurística, IP *Defragmentation*, remontagem de pacotes de TCP e bloqueio de pacotes malformados;

3.21.24. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;

3.21.25. Possuir assinaturas para bloqueio de ataques de *buffer overflow*;

3.21.26. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;

3.21.27. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS e Anti-Spyware, permitindo a criação de exceções com granularidade nas configurações;

3.21.28. Permitir o bloqueio de vírus e *spywares* em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;

3.21.29. Suportar bloqueio de arquivos por tipo;

3.21.30. Identificar e bloquear comunicação com *botnets*;

3.21.31. Deve suportar várias técnicas de prevenção, incluindo *Drop* e *tcp-rst* (Cliente, Servidor e ambos);

3.21.32. Deve suportar referência cruzada com CVE;

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

- 3.21.33.1.** O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 3.21.34.** Deve suportar a captura de pacotes (PCAP) por assinatura de IPS;
- 3.21.35.** Deve permitir que na captura de pacotes por assinaturas de IPS seja definido o número de pacotes a serem capturados. Esta captura deve permitir selecionar, no mínimo, 50 pacotes;
- 3.21.36.** Deve possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos sejam resolvidas pelo Firewall com endereços (IPv4 e IPv6), previamente definidos;
- 3.21.37.** Os eventos devem identificar o país de onde partiu a ameaça;
- 3.21.38.** Deve incluir proteção contra vírus em conteúdo HTML e Java script, software espião (Spyware) e worms;
- 3.21.39.** Proteção contra downloads involuntários usando HTTP de arquivos executáveis;
- 3.21.40.** Rastreamento de vírus em pdf;
- 3.21.41.** Deve permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, etc.);
- 3.21.42.** Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.
- 3.21.43.** A prevenção de ameaças deverá ser integrada no próprio appliance de NGFW, não sendo aceito quaisquer componentes adicionais com esta função.

3.22. ANÁLISE DE MALWARE

- 3.22.1.** Devido aos *Malwares* hoje em dia serem muito dinâmicos e um antivírus comum reativo não ser capaz de detectar os mesmos com a mesma velocidade que suas variações são criadas, a solução ofertada deve possuir funcionalidades para análise de Malwares não conhecidos incluídas na própria ferramenta ou entregue com composição com outro fabricante sem custo adicional;
- 3.22.2.** O dispositivo de proteção deve ser capaz de enviar arquivos trafegados de forma automática para análise "*In Cloud*" ou local, onde o arquivo será executado e simulado em ambiente controlado;
- 3.22.3.** Selecionar através de políticas granulares quais tipos de arquivos sofrerão esta análise incluindo, mas não limitado a: endereço IP de origem/destino, usuário/grupo do AD/LDAP, aplicação, porta, URL/categoria de URL de destino, tipo de arquivo e todas estas opções simultaneamente;
- 3.22.4.** Deve possuir a capacidade de diferenciar arquivos analisados em pelo menos três categorias: malicioso, não malicioso e suspeito;
- 3.22.5.** Suportar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Android, MacOS, Windows 8, Windows 7 (32 bits) e Windows 7 (64 bits), Windows 10 (32 bits) e Windows 10 (64 bits);
- 3.22.6.** Deve suportar a monitoração de arquivos trafegados na internet (HTTPs, FTP, HTTP, SMTP) como também arquivos trafegados internamente entre servidores de arquivos usando SMB em todos os modos de implementação: *sniffer*, transparente e L3;
- 3.22.7.** Para ameaças trafegadas em protocolo SMTP e POP3, a solução deve ter a capacidade de mostrar nos relatórios o remetente, destinatário e assunto dos e-mails permitindo identificação ágil do usuário vítima do ataque;
- 3.22.8.** O sistema de análise "*In Cloud*" ou local deve gerar assinaturas de Antivírus e *Anti-Spyware* automaticamente, definir URLs não confiáveis utilizadas pelo novo Malware e prover informações sobre o usuário infectado (seu endereço ip e seu *login de rede*);
- 3.22.9.** Caso a solução seja fornecida em *appliance* local, deve possuir, no mínimo, 28 ambientes controlados (*Sandbox*) independentes para execução simultânea de arquivos suspeitos;
- 3.22.10.** Caso seja necessário, licenças de sistemas operacional e softwares para execução de arquivos no ambiente controlado (*Sandbox*), as mesmas devem ser fornecidas em sua totalidade, sem custos adicionais para a contratante;
- 3.22.11.** Suportar a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado;
- 3.22.12.** Deve atualizar a base com assinaturas para bloqueio dos malwares identificados em *Sandbox* com frequência;
- 3.22.13.** A análise de Malware deverá ser integrada no próprio appliance de NGFW, não sendo aceito quaisquer componentes adicionais com esta função.

3.23. FILTRO URL

3.23.1. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

3.23.2. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, Ips, Redes e Zonas de segurança;

3.23.3. Incluir nativamente *Explicit Web Proxy* e *proxy Web* transparente;

3.23.4. Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via *ldap*, *Active Directory*, base de dados local, inclusive em modo de proxy transparente e explícito;

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

3.23.6. Suporta a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;

3.23.7. Deve bloquear o acesso a sites de busca (Google, Bing e Yahoo). O Firewall deve ter mecanismo que implemente a navegação com o uso o *Safe Search*, independente da intervenção do usuário.

3.23.8. Suporta base ou cache de URLs local no *appliance*, evitando *delay* de comunicação/validação das URLs;

3.23.9. Possui pelo menos 60 categorias de URLs;

3.23.10. A categorização de URL deve analisar toda a URL e não somente até o nível de diretório;

3.23.11. Suporta a criação categorias de URLs customizadas;

3.23.12. Suporta a criação de exceções nos bloqueios de filtro de URLs;

3.23.13. Permite a customização de página de bloqueio;

3.23.14. Permite o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão "Continuar" para permitir o usuário continuar acessando o site);

3.23.15. A funcionalidade de Filtro de URL, categorizada localmente, deve operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;

3.23.16. Suporta a inclusão nos logs do produto de informações das atividades dos usuários;

3.23.17. Deve possuir base ou cache de URLs local no *appliance* ou em nuvem do próprio fabricante, evitando *delay* de comunicação/validação das URLs;

3.23.18. Deve salvar nos logs as informações dos seguintes campos do cabeçalho HTTP nos acessos a URLs: UserAgent, Referer, e X-Forwarded For;

3.24. IDENTIFICAÇÃO DE USUÁRIOS

3.24.1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, *Active Directory*, e base de dados local;

3.24.2. Deve possuir integração com Microsoft *Active Directory* e LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

3.24.3. Deve possuir integração com *Radius* para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

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

3.24.5. Suporte a autenticação *Kerberos*;

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

3.24.7. Deve identificar usuários através de leitura do campo nos logs do firewall o endereço IP, bem como o usuário de rede responsável pelo acesso;

3.24.8. Deve permitir a criação de políticas de segurança baseadas em usuários de rede com reconhecimento dos mesmos através de leitura do campo de identificação do usuário;

3.24.9. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;

3.24.10. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em servidores acessados remotamente, mesmo que não sejam servidores Windows;

3.25. QOS

- 3.25.1.** Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, Ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming;
- 3.25.2.** Suportar a criação de políticas de QoS e traffic-shaping por:
- 3.25.2.1.** *Endereço de origem;*
- 3.25.2.2.** *Endereço de destino;*
- 3.25.2.3.** *Por usuário e grupo do LDAP/AD;*
- 3.25.2.4.** *Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;*
- 3.25.2.5.** *Por porta.*
- 3.25.3.** QoS deve possibilitar a definição de classes por:
- 3.25.3.1.** *Banda Garantida;*
- 3.25.3.2.** *Banda Máxima;*
- 3.25.3.3.** *Fila de Prioridade.*
- 3.25.4.** Suportar priorização Real Time de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype;
- 3.25.5.** Suportar marcação de pacotes *Diffserv*, inclusive por aplicação;
- 3.25.6.** Deve implementar QoS (*traffic-shaping*), para pacotes marcados por outros ativos na rede (DSCP). A priorização e limitação do tráfego deve ser efetuada nos dois sentidos da conexão (*Inbound e Outbound*);
- 3.25.7.** Disponibilizar estatísticas Real Time para classes de QoS;
- 3.25.8.** Deve suportar QoS (*traffic-shaping*), em interface agregadas;
- 3.25.9.** Deverá permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.

3.26. FILTRO DE DADOS

- 3.26.1.** Permite a criação de filtros para arquivos e dados pré-definidos;
- 3.26.2.** Os arquivos devem ser identificados por extensão, tipo e assinaturas (ou *fingerprint*);
- 3.26.3.** Permite identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, SMTP, POP3, IMAP, MAPI, FTP e NNTP);
- 3.26.4.** Suportar identificação de arquivos compactados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
- 3.26.5.** Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.

3.27. GEOLOCALIZAÇÃO

- 3.27.1.** Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;
- 3.27.2.** Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
- 3.27.3.** Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas.

3.28. VPN

- 3.28.1.** Suportar VPN Site-to-Site e Cliente-To-Site;
- 3.28.2.** Suportar IPSec VPN;
- 3.28.3.** Suportar SSL VPN;
- 3.28.4.** A VPN IPSec deve suportar:
- 3.28.5.** *DES e 3DES;*
- 3.28.6.** *Autenticação MD5 e SHA-1;*
- 3.28.7.** *Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;*
- 3.28.8.** *Algoritmo Internet Key Exchange (IKEv1 e v2);*
- 3.28.9.** *AES 128, 192 e 256 (Advanced Encryption Standard);*
- 3.28.10.** *Autenticação via certificado IKE PKI.*
- 3.28.11.** Deve possuir interoperabilidade com os seguintes fabricantes: Palo Alto Networks, Cisco, Check Point, Juniper, Fortinet, SonicWall;

3.28.12. Deve permitir habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de troubleshooting;

3.28.13. VPN SSL deve suportar:

3.28.13.1. Usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;

3.28.13.2. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente. Caso necessite de agente, deve estar licenciada para ou suportar sem o uso de licença, 50 (cinquenta) clientes de VPN SSL simultâneos;

3.28.13.3. Atribuição de endereço IP nos clientes remotos de VPN SSL;

3.28.13.4. Deve permitir a atribuição de IPs fixos nos usuários remotos de VPN SSL.

3.28.14. Deve permitir a criação de rotas de acesso e faixas de endereços IP atribuídas a clientes remotos de VPN de forma customizada por usuário AD/LDAP e grupo de usuário AD/LDAP;

3.28.15. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;

3.28.16. Atribuição de DNS nos clientes remotos de VPN;

3.28.17. Deve suportar autenticação de clientes VPN a partir de diferentes sistemas operacionais remotos (Android, IOS, Mac Windows e Chrome OS);

3.28.18. A solução de VPN deve verificar se o client que está conectando é o mesmo para o qual o certificado foi emitido inicialmente. O acesso deve ser bloqueado caso o dispositivo não seja o correto;

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

3.28.20. Suportar autenticação via AD/LDAP, OTP (One Time Password), certificado e base de usuários local;

3.28.21. Suporta leitura e verificação de CRL (certificate revocation list);

3.28.22. Permite a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;

3.28.23. Agente deverá comunicar-se com o portal para determinar as políticas de segurança do usuário;

3.28.24. Deve permitir que a conexão com a VPN SSL seja estabelecida das seguintes formas:

3.28.24.1. Antes do usuário autenticar na estação;

3.28.24.2. Após autenticação do usuário na estação;

3.28.24.3. Sob demanda do usuário.

3.28.25. Deverá manter uma conexão segura com o portal durante a sessão;

3.28.26. O agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows 7, Windows 8 e Mac Osx.

3.29. COMPATIBILIDADE

3.29.1. Todos os itens de hardware e software fornecidos pela PROPONENTE deverão ser da mesma marca e fabricante. A padronização da marca garante que os equipamentos adquiridos sejam 100% compatíveis entre si, permitindo a proteção de investimento a ser realizado por este órgão. Desta forma, faz-se necessária a aquisição de produtos de mesma marca e fabricante, com o fim de garantir a interoperabilidade e possibilidade de operar em Alta Disponibilidade entre si.

3.30. LICENCIAMENTO

3.30.1. Deve ser fornecido com a versão de software mais recente disponível para o equipamento;

3.30.2. Deve ser fornecido com todas as licenças de software necessárias para o funcionamento de todos os recursos descritos e exigidos neste termo para o prazo mínimo de 05 anos.

3.31. GARANTIA E SUPORTE

3.31.1. Durante o prazo de 05 anos, deve ser possível realizar a atualização de sistema operacional dos equipamentos, incluindo atualizações de novas assinaturas;

3.31.2. A garantia deve incluir envio de peças ou equipamentos de reposição nos locais especificados neste termo de referência, obedecendo a modalidade NBD (Next Business Day);

3.31.3. Os chamados poderão ser abertos diretamente com o fabricante ou autorizada pelo fabricante através de ligação telefônica 0800 no idioma Português, bem como via website e/ou e-mail durante a vigência da garantia (5 anos), sendo tais canais de comunicação informados pela CONTRATADA, por ocasião da assinatura da ARP/Contrato, indicando a empresa que prestará os serviços de garantia, com todas as informações necessárias (endereço completo, telefone, fax, e-mail e, se houver, responsável

técnico) através de declaração assinada pelo representante legal da mesma, específica para este pregão. A substituição da empresa indicada para a prestação da garantia on-site somente poderá ser feita mediante comunicação e autorização prévia do Ministério Público do Estado do Pará.

3.31.4. O suporte deverá ser na modalidade de 24x7 (24 horas por dia, 7 dias por semana), com atendimento através de ligação telefônica para atendimentos emergenciais.

3.32. DOS ITENS DO LOTE 01

3.32.1. Item 01 - NGFW de pequeno porte com SD-WAN integrada, garantia, suporte e todas as licenças necessárias: 134 (cento e trinta e quatro) unidades.

3.32.1.1. CAPACIDADE E QUANTIDADE

3.32.1.1.1. Throughput de, no mínimo, 02 (dois) Gbps com a funcionalidade de firewall habilitada;

3.32.1.1.2. Throughput de no mínimo 450 (quatrocentos e cinquenta) Mbps com a funcionalidade de controle de aplicação e logs habilitada;

3.32.1.1.3. Throughput de no mínimo 160 (cento e sessenta) Mbps com as seguintes funcionalidades habilitadas: controle de aplicação, IPS, Antivírus e Anti-Spyware e log. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, todas deverão ter valor superior ao throughput requerido;

3.32.1.1.4. Capacidades (throughput) comprovadas por documento de domínio público disponibilizado pelo fabricante, não sendo admitida a comprovação de Throughput para funcionalidades de camada 7 (Controle de Aplicação e IPS, por exemplo), com tráfego UDP e/ou RFCs baseadas neste protocolo;

3.32.1.1.5. Efetividade de Segurança mínima de 80%, classificados como recomendado em Security Value Map (SVM) Comparative Report para Next Generation Firewall (NGFW) da NSSSLabs ou certificação ICSA Labs para o ano de 2018 ou posterior, seja para o modelo apresentado ou para equipamento da mesma linha que possua mesmo sistema operacional e engine de anti-vírus, comprovada por documento de domínio público;

3.32.1.1.6. Suporte a, no mínimo, 192 (Cento e noventa e dois) mil conexões simultâneas;

3.32.1.1.7. Suporte a, no mínimo, 13 (treze) mil novas conexões por segundo;

3.32.1.1.8. Fonte de alimentação automática 100-240V AC;

3.32.1.1.9. Possuir espaço em disco SSD interno com no mínimo 32 (trinta e dois) GB;

3.32.1.1.10. No mínimo 7 (sete) interfaces de rede gigabit Ethernet RJ45, devendo ser possível configurar ao menos 02 (duas) destas interfaces como WAN;

3.32.1.1.11. 01 (uma) interface do tipo console ou similar;

3.32.1.1.12. Suporte a, no mínimo, 20 (vinte) zonas de segurança;

3.32.1.1.13. Estar licenciada para suportar sem o uso de licença, 200 (duzentos) clientes de VPN SSL simultâneos;

3.32.1.1.14. Estar licenciada para suportar sem o uso de licença, 200 (duzentos) túneis de VPN IPSEC simultâneos.

3.32.2. Item 02 - NGFW de médio porte com SD-WAN integrada, garantia, suporte e todas as licenças necessárias: 20 (vinte) unidades

3.32.2.1. CAPACIDADE E QUANTIDADE

3.32.2.1.1. Throughput de, no mínimo, 10 (dez) Gbps com a funcionalidade de firewall habilitada;

3.32.2.1.2. Throughput de no mínimo 02 (dois) Gbps com a funcionalidade de controle de aplicação e logs habilitada;

3.32.2.1.3. Throughput de no mínimo 700 (setecentos) Mbps com as seguintes funcionalidades habilitadas simultaneamente: controle de aplicação IPS, Antivírus e Anti-Spyware e logs. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, todas deverão ter valor superior ao throughput requerido;

3.32.2.1.4. Capacidades (throughput) comprovadas por documento de domínio público disponibilizado pelo fabricante, não sendo admitida a comprovação de Throughput para funcionalidades de camada 7 (Controle de Aplicação e IPS, por exemplo), com tráfego UDP e/ou RFCs baseadas neste protocolo;

3.32.2.1.5. Efetividade de Segurança mínima de 80%, classificados como recomendado em Security Value Map (SVM) Comparative Report para Next Generation Firewall (NGFW) da NSSSLabs ou certificação ICSA Labs para o ano de 2018 ou posterior, seja para o modelo apresentado ou para equipamento da mesma linha que possua mesmo sistema operacional e engine de anti-vírus,

comprovada por documento de domínio público; Suporte a, no mínimo, 1,5 (um vírgula cinco) milhão de conexões simultâneas;

3.32.2.1.6. Suporte a, no mínimo, 50 (cinquenta) mil novas conexões por segundo;

3.32.2.1.7. Fonte de alimentação automática 100-240V AC;

3.32.2.1.8. Possuir espaço em disco SSD interno com no mínimo 240 (duzentos e quarenta) GB;

3.32.2.1.9. No mínimo 10 (dez) interfaces de rede gigabit Ethernet RJ45, devendo ser possível configurar ao menos 02 (duas) destas interfaces como WAN;

3.32.2.1.10. No mínimo 08 (oito) slots SFP;

3.32.2.1.11. No mínimo 02 (dois) slots SFP+;

3.32.2.1.12. 01 (uma) interface do tipo console ou similar;

3.32.2.1.13. Fonte de alimentação automática 100-240V AC;

3.32.2.1.14. Suporte a, no mínimo, 06 (seis) sistemas virtuais lógicos (Contextos) no firewall físico. Os contextos virtuais devem suportar as funcionalidades nativas do gateway de proteção incluindo: Firewall, IPS, Antivírus, Anti-Spyware, Filtro de URL, Filtro de Dados, VPN, Controle de Aplicações, QoS, NAT e Identificação de usuários;

3.32.2.1.15. Suporte a, no mínimo, 50 (cinquenta) zonas de segurança;

3.32.2.1.16. Estar licenciada para ou suportar sem o uso de licença, 400 (quatrocentos) clientes de VPN SSL simultâneos;

3.32.2.1.17. Estar licenciada para ou suportar sem o uso de licença, 02 (dois) mil túneis de VPN IPSEC simultâneos.

3.32.3. Item 03 - NGFW concentrador de VPN com SD-WAN integrada, garantia, suporte e todas as licenças necessárias: 02 (duas) unidades em HA (Alta Disponibilidade)

3.32.3.1. CAPACIDADE E QUANTIDADE

3.32.3.1.1. Throughput de, no mínimo, 36 (trinta e seis) Gbps com a funcionalidade de firewall habilitada;

3.32.3.1.2. Throughput de no mínimo 15 (quinze) Gbps com a funcionalidade de controle de aplicação habilitada;

3.32.3.1.3. Throughput de no mínimo 07 (sete) Gbps com as seguintes funcionalidades habilitadas simultaneamente: controle de aplicação IPS, Antivírus e Anti-Spyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, todas deverão ter valor superior ao throughput requerido;

3.32.3.1.4. Capacidades (throughput) comprovadas por documento de domínio público disponibilizado pelo fabricante, não sendo admitida a comprovação de Throughput para funcionalidades de camada 7 (Controle de Aplicação e IPS, por exemplo), com tráfego UDP e/ou RFCs baseadas neste protocolo;

3.32.3.1.5. Efetividade de Segurança mínima de 80%, classificados como recomendado em Security Value Map (SVM) Comparative Report para Next Generation Firewall (NGFW) da NSS Labs ou certificação ICSA Labs para o ano de 2018 ou posterior, seja para o modelo apresentado ou para equipamento da mesma linha que possua mesmo sistema operacional e engine de anti-vírus, comprovada por documento de domínio público;

3.32.3.1.6. Suporte a, no mínimo, 7,5 (sete vírgula cinco) milhões de conexões simultâneas;

3.32.3.1.7. Suporte a, no mínimo, 280 (duzentos e oitenta) mil novas conexões por segundo;

3.32.3.1.8. Fontes de alimentação automáticas 100-240V AC, redundante;

3.32.3.1.9. Possuir espaço em disco SSD interno com no mínimo 240 (duzentos e quarenta) GB;

3.32.3.1.10. No mínimo 08 (oito) interfaces de rede gigabit Ethernet RJ45, devendo ser possível configurar ao menos 02 (duas) destas interfaces como WAN;

3.32.3.1.11. No mínimo 06 (seis) slots SFP;

3.32.3.1.12. No mínimo 02 (dois) slots SFP+;

3.32.3.1.13. 01 (uma) interface do tipo console ou similar;

3.32.3.1.14. Suporte a, no mínimo, 06 (seis) sistemas virtuais lógicos (Contextos) no firewall físico. Os contextos virtuais devem suportar as funcionalidades nativas do gateway de proteção incluindo: Firewall, IPS, Antivírus, Anti-Spyware, Filtro de URL, Filtro de Dados, VPN, Controle de Aplicações, QoS, NAT e Identificação de usuários;

3.32.3.1.15. Suporte a, no mínimo, 100 (cem) zonas de segurança;

3.32.3.1.16. Estar licenciada para suportar sem o uso de licença, 09 (nove) mil clientes de VPN SSL simultâneos;

3.32.3.1.17. Estar licenciada para suportar sem o uso de licença, 02 (dois) mil túneis de VPN IPSEC simultâneos.

3.32.4. Item 04 - SISTEMA DE GERÊNCIA CENTRALIZADA

3.32.4.1. Deve prover gestão centralizada dos dispositivos denominados PONTOS DE PRESENÇA, e ser necessariamente do mesmo fabricante do NGFW;

3.32.4.2. Por console de gerência, entende-se as licenças de software necessárias para esta funcionalidade;

3.32.4.3. Deve estar licenciado e suportar a gestão de, no mínimo, 160 (cento e sessenta) dispositivos denominados PONTOS DE PRESENÇA;

3.32.4.4. Deve ser do tipo Appliance Físico, Appliance Virtual ou solução de software baseada em máquina virtual (VM). Caso seja baseada em Máquina Virtual (VM), a PROPONENTE deverá indicar em sua proposta qual a necessidade de hardware a ser disponibilizada pelo CONTRATANTE para a respectiva instalação;

3.32.4.5. Caso seja em VM, deve ser compatível com VMware ESX(i);

3.32.4.6. Possuir ao menos 4 (quatro) interfaces de rede VNIC;

3.32.4.7. Deve estar licenciado para suporta ao menos 5GB Log/dia + 1TB (Cinco Gigabyte de Log por dia e 01 Terabyte);

3.32.4.8. Deve suportar operação em alta disponibilidade (há) sincronizando as mudanças na base de dados entre as estações de gerência;

3.32.4.9. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;

3.32.4.10. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;

3.32.4.11. Permitir acesso concorrente de administradores;

3.32.4.12. Possuir interface baseada em linha de comando para administração da solução de gerência;

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

3.32.4.14. Bloqueio de alterações, no caso de acesso simultâneo de dois ou mais administradores;

3.32.4.15. Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;

3.32.4.16. Gerar alertas automáticos via Email;

3.32.4.17. Gerar alertas automáticos via SNMP;

3.32.4.18. Deve suportar backup/restore de todas as configurações da solução de gerência, permitindo ao administrador agendar backups da configuração em um determinado dia e hora;

3.32.4.19. Deve ser permitido ao administrador transferir os backups para um servidor FTP;

3.32.4.20. As alterações realizadas em um servidor de gerência deverão ser automaticamente replicadas para o servidor redundante;

3.32.4.21. Deve ser permitido aos administradores se autenticarem nos servidores de gerência através de contas de usuários LOCAIS;

3.32.4.22. Deve ser permitido aos administradores se autenticarem nos servidores de gerência através de usuários de base externa LDAP;

3.32.4.23. Deve ser permitido aos administradores se autenticarem nos servidores de gerência através de base externa RADIUS;

3.32.4.24. Deve ser permitido aos administradores se autenticarem nos servidores de gerência através de Certificado Digital X.509 (PKI);

3.32.4.25. Deve suportar sincronização do relógio interno via protocolo NTP;

3.32.4.26. Deve registrar as ações efetuadas por quaisquer usuários;

3.32.4.27. Devem ser fornecidos manuais de instalação, configuração e operação de toda a solução, na língua portuguesa ou inglesa, com apresentação de boa qualidade;

3.32.4.28. Suportar SNMP versão 2 e versão 3 nos equipamentos de gerência;

3.32.4.29. Deve permitir virtualizar a solução de gerência, de forma que cada administrador possa gerenciar, visualizar e editar apenas os dispositivos autorizados e cadastrados no seu ambiente virtualizado;

3.32.4.30. A solução de gerência deve permitir criar administradores que tenham acesso à todas as instâncias de virtualização;

- 3.32.4.31. Deve suportar XML API;
- 3.32.4.32. O gerenciamento deve possibilitar a criação e administração de políticas de firewall e controle de aplicação;
- 3.32.4.33. O gerenciamento deve possibilitar a criação e administração de políticas de IPS, Antivírus e Anti-Spyware;
- 3.32.4.34. O gerenciamento deve possibilitar a criação e administração de políticas de Filtro de URL;
- 3.32.4.35. Permitir localizar quais regras um objeto está sendo utilizado;
- 3.32.4.36. Deve atribuir sequencialmente um número a cada regra de firewall;
- 3.32.4.37. Deve atribuir sequencialmente um número a cada regra de DOS;
- 3.32.4.38. Permitir criação de regras que fiquem ativas em horário definido;
- 3.32.4.39. Permitir backup das configurações e rollback de configuração para a última configuração salva;
- 3.32.4.40. Deve possuir mecanismo de Validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);
- 3.32.4.41. Deve possibilitar a visualização e comparação de configurações atuais, configuração anterior e configurações antigas;
- 3.32.4.42. Deve permitir que todos os firewalls sejam controlados de forma centralizada utilizando apenas um servidor de gerência;
- 3.32.4.43. O servidor de gerência deve ser hospedado em um equipamento independente, não exercendo funções de firewall;
- 3.32.4.44. A solução deve incluir uma ferramenta para gerenciar centralmente as licenças de todos os appliances controlados pela estação de gerenciamento, permitindo ao administrador atualizar licenças nos appliances através dessa ferramenta;
- 3.32.4.45. A solução deve possibilitar a distribuição e instalação remota, de maneira centralizada, de novas versões de software dos appliances;
- 3.32.4.46. Deve ser capaz de gerar relatórios ou exibir comparativos entre duas sessões diferentes, resumindo todas as alterações efetuadas;
- 3.32.4.47. Permitir visualizar, a partir da estação de gerência centralizada, informações detalhadas dos dispositivos gerenciados, tais como hostname, serial, IP de gerência, licenças, horário do sistema e firmware;
- 3.32.4.48. Permitir criar os objetos que serão utilizados nas políticas de forma centralizada.

3.32.5. Item 05 - Serviço de Instalação/Configuração

- 3.32.5.1. Os equipamentos concentradores e o Sistema de Gerência Centralizada devem ser instalados no prédio sede do Ministério Público do Pará - MPPA (Rua João Diogo, nº 100 – Cidade Velha - 66.015.165 Belém/PA). Além dos equipamentos e sistema citados acima, este item contempla a instalação de um NGFW em cada uma das unidades relacionadas no Anexo H **Anexo I do TR - Localidades**;
- 3.32.5.2. Reunião inicial: deverá ser realizada uma reunião inicial entre o gestor do contrato e a PROPONENTE, cuja pauta observará, pelo menos:
 - 3.32.5.2.1. Assinatura da Carta de Confidencialidade;
 - 3.32.5.2.2. Esclarecimentos relativos a questões operacionais e de gerenciamento do contrato;
 - 3.32.5.2.3. Estrutura organizacional da CONTRATANTE;
 - 3.32.5.2.4. Infraestrutura de TI da CONTRATANTE;
- 3.32.5.3. A CONTRATADA deverá prestar serviços de instalação e configuração, que compreendem, entre outros, os seguintes procedimentos:
 - 3.32.5.3.1. Análise da topologia e arquitetura da rede, considerando os roteadores, servidores de aplicação e firewall já existentes e instalados;
 - 3.32.5.3.2. Análise do acesso Internet, sites remotos, serviços de rede oferecidos aos funcionários e aos usuários externos;
 - 3.32.5.3.3. Regras de Firewall existentes e aplicáveis solução ofertada dada a colocação desta na Rede deste parquet;
 - 3.32.5.3.4. Análise do posicionamento de qualquer outro equipamento ou sistema relevante na segurança de qualquer perímetro protegido pela solução;
 - 3.32.5.3.5. Apresentação do plano de implantação com o descritivo de todos os serviços a serem executados e topologia física e lógica a ser implementada;

3.32.5.3.6. Configuração do sistema de Firewall, SD-WAN, VPN, IPS, Filtro URL, Antivírus e Anti-Malware de acordo com as exigências levantadas com as devidas atualizações necessárias;

3.32.5.3.7. Instalação de Sistema de Gerência Centralizada em Appliance Físico, Appliance Virtual ou solução baseada em VM (máquina virtual), de acordo com a oferta da CONTRATADA. O mesmo será considerado entregue, quando for instalado e configurado na sede do MPPA, com todas as atualizações, configurações e licenças. Deverão ser adicionados a este todos os pontos de presença do Anexo **I do TR (Localidades)** e Concentradores, cujos deverão estar sendo monitorados e gerenciados por este Sistema de Gerência Centralizada;

3.32.5.4. Deve haver geração de relatório e entrega da documentação da instalação com as configurações efetuadas e as decisões tomadas, diagramas e topologias em formato legível e tecnicamente fundamentado;

3.32.5.5. O recebimento definitivo consiste no aceite dos produtos e/ou serviços além do atendimento aos termos e condições do Edital, Contrato e seus anexos, inclusive a proposta comercial da PROPONENTE.

3.32.5.6. O aceite poderá ser parcial, ou seja, se acordo com a entrega de cada item adquirido.

3.32.6. Item 06 - Treinamento “Hands On” sobre Solução de Firewall/SD-WAN

3.32.6.1. A CONTRATADA deverá ministrar treinamento do tipo “Hands On” sobre a solução de Firewall/SD-WAN adquirida, incluindo instalação, configuração básica e avançada, troubleshoot, monitoramento e gerenciamento;

3.32.6.2. A carga horária mínima será de 20 horas divididas em expedientes de 4h/dia, das 8h às 12h;

3.32.6.3. O treinamento será ministrado para um total de seis (6) participantes do quadro de pessoal do Ministério Público definidos pela CONTRATANTE;

3.32.6.4. O repasse deverá ter caráter prático e se baseará no sistema Firewall/SD-WAN efetivamente instalado na CONTRATANTE;

3.32.6.5. O treinamento deve ser do tipo presencial e a sua realização será na cidade de Belém (Pará) nas dependências do Ministério Público. A CONTRATANTE irá ceder uma sala, um projetor e computadores, com acesso à internet, para sua realização. É de responsabilidade da CONTRATADA designar um profissional certificado pelo Fabricante, fornecer todo material audiovisual, didático e, caso necessário, outros equipamentos eletrônicos para a realização dos treinamentos, além de impressos. Todos os demais custos, ônus, obrigações e encargos para o treinamento devem ser arcados pela CONTRATADA.

4 PRAZO E CONDIÇÕES DE EXECUÇÃO, RECEBIMENTO E ENTREGA

4.1. CONTRATADA se compromete a efetuar a entrega dos produtos solicitados no prazo não superior a 60 (sessenta) dias corridos, a contar do início da vigência do contrato ou do recebimento nota de empenho, no caso desta substituir o contrato.

4.2. A entrega dos produtos será no Edifício Sede do Ministério Público, sito na Rua João Diogo, n. 100 – 2º andar, Cidade Velha, Belém, Pará, no horário das 08h00min às 14h00min, de segunda a sexta-feira, exceto nos feriados e dias facultativos, correndo por conta da contratada todas as despesas de embalagem, seguros, transporte, tributos, encargos trabalhistas e previdenciários, decorrentes do serviço e equipamentos necessários para o seu funcionamento, devendo a entrega ser agendada, com até 48h de antecedência, pelos telefones (91) 4006-3480/3481;

4.3. O CONTRATADO terá prazo de 06 (seis) dias úteis a contar da comunicação para retirar a Nota de Empenho de Despesas ou instrumento equivalente.

4.4. Os equipamentos deverão ser novos (de primeiro uso), e deverão ser entregues devidamente protegidos e adequadamente embalados contra danos de transporte manuseio e acompanhados das notas fiscais de remessa;

4.5. O MINISTÉRIO PÚBLICO poderá solicitar, de acordo com a demanda Institucional e mediante Nota de Empenho, a quantidade necessária ao seu consumo regular;

4.6. Os detentores da Ata de Registro de Preços ficam obrigados a atender todos os pedidos de fornecimento efetuados pelo ÓRGÃO durante a vigência da Ata, mesmo que a entrega deles decorrentes esteja prevista para data posterior ao seu vencimento;

4.7. Caso se veja impossibilitada de cumprir com o prazo estipulado no item 4.1, a Contratada deverá, por escrito e com antecedência mínima de 10 (dez) dias corridos antes de expirado o prazo, solicitar prorrogação do prazo e apresentar justificativas;

4.8. O pedido de prorrogação, com indicação do novo prazo, quando for o caso, deverá ser encaminhado à fiscalização da Contratante, que poderá, de modo justificado, acolher ou não o pedido;

4.9. Vencidos os prazos de entrega ou de prorrogação e não cumprida a obrigação de entrega, a Contratante oficiará a Contratada acerca do transcurso da data limite, passando o inadimplemento, a partir daí, a ser considerado como recusa do cumprimento da obrigação pactuada e, por conseguinte, sujeitando a empresa às penalidades prevista na lei;

4.10. O recebimento do objeto pela FISCALIZAÇÃO ou COMISSÃO DE RECEBIMENTO (nas compras acima de R\$ 80.000,00) se dará em duas etapas:

a) Em caráter provisório, imediatamente após a entrega **de material dos equipamentos (item 1 a 3) e serviços (itens 4 a 6)**, representada pela conferência da quantidade e da qualidade do material entregue (esta em sentido da aparência da embalagem) e conformidade com o modelo indicado na proposta comercial, **com a entrega do sistema e verificação da conformidade com as informações prestadas na proposta comercial, o funcionamento básico dos equipamentos instalados e a conclusão da carga-horária do treinamento;**

b) Definitivamente, em até 10 (dez) dias úteis a contar do recebimento provisório, mediante análise individual, que comprove sua conformidade com os padrões estabelecidos no presente Edital;

c) Os objetos licitados serão recebidos e conferidos pela Fiscalização/Comissão de Recebimento designada por esta Instituição.

4.11. O objeto adjudicado somente será considerado entregue quando emitido o Termo de Recebimento Definitivo dos Bens pela Contratante;

4.12. A LICITANTE deve fornecer em sua proposta comercial a lista de PART NUMBERS do fabricante e suas respectivas quantidades necessárias para atender as características técnicas solicitadas neste edital;

4.13. Se, após o recebimento provisório, constatar-se que os equipamentos foram entregues em desacordo com o solicitado, fora da especificação ou incompletos, após a notificação à Contratada, será suspenso o pagamento até que sanada a situação, independente de aplicação de sanções cabíveis;

4.14. O recebimento do material não exclui a responsabilidade administrativa, civil e penal da empresa por problemas causados durante o uso dos itens adquiridos nem exclui a responsabilidade da CONTRATADA pelo perfeito desempenho do objeto fornecido, cabendo-lhe sanar quaisquer irregularidades detectadas quando de sua utilização;

4.15. A Contratada e/ou detentora da ata deve promover, às suas expensas, a substituição total ou parcial do objeto que apresentar qualquer irregularidade;

4.16. Em caso de qualquer inconformidade, a Contratada terá prazo máximo de 30 (trinta) dias corridos após notificação emitida pela Contratante para sanar quaisquer pendências encontradas, sob pena de aplicação das sanções cabíveis;

4.17. Na hipótese de ser verificada a impropriedade do material no ato da entrega, o mesmo será imediatamente rejeitado, no todo ou em parte, a critério da FISCALIZAÇÃO responsável pelo recebimento, sendo o fornecedor notificado a proceder à substituição no prazo máximo de 30 (trinta) dias corridos, contados da ciência da rejeição, sendo-lhe, ainda, concedidos 05 (cinco) dias úteis para retirada do material ou parte do que foi rejeitado;

4.18. Os profissionais responsáveis pela implantação da solução e treinamento devem ser certificados pelo fabricante da solução;

4.19. A Contratada deverá promover, às suas expensas, a substituição total ou parcial do objeto que apresentar qualquer irregularidade.

4.20. O prazo de garantia será de, no mínimo, 60 (SESSENTA) meses, contados a partir da data do aceite definitivo. A garantia será prestada on-site na sede do MP/PA.

4.21. Os serviços de garantia e suporte técnicos deverão ser prestados aos equipamentos existentes nas dependências do Departamento de Informática – Edifício Sede do MP/PA, 2º Andar, Rua João Diogo, 100, Cidade Velha, Belém, Pará, CEP 66.015.165, assegurando-se, sem ônus para o CONTRATANTE, a cobertura para defeitos de fabricação, pelo período mínimo de 60 (Sessenta) meses, englobando equipamentos, peças e serviços, contados da data em que ocorrer o recebimento definitivo dos bens;

4.22. Durante a vigência dos serviços, chamados técnicos, sem limite de quantidade, poderão ser abertos, no horário de 00:00 às 23:59 horas, de segunda-feira a domingo, via discagem direta gratuita (linha 0800), ou via sistema próprio, em sítio na Internet, caracterizando a abertura do chamado;

4.23. O suporte técnico, deverão ser mantidas pelo prazo definido nas especificações de cada item;

- 4.24.** Os serviços de Suporte e Garantia do equipamento devem ser em regime de 5x8xNBD, modalidade Next Business Day (próximo dia útil comercial), durante o período mínimo de 60 (sessenta) meses para toda a solução, contados da data em que ocorrer recebimento definitivo dos bens;
- 4.25.** O uso da modalidade remota não afeta de forma alguma a contagem dos prazos estipulados;
- 4.26.** O problema dos equipamentos defeituosos, caso comprovado, deverá ser sanado dentro dos tempos estipulados. Quando não for possível solucionar o problema no prazo estipulado, caso autorizado após avaliação por representante do Departamento de Informática, deverá ser fornecido outro equipamento de igual configuração ou superior, até resolução definitiva do problema;
- 4.27.** A CONTRATADA, no momento da assinatura da ARP/Contrato, deverá fornecer número de telefone e/ou endereço de site na internet da central de atendimento para abertura de chamados;
- 4.28.** Os chamados deverão ser resolvidos em até 3 (três) dias úteis, contados do primeiro dia útil seguinte à abertura do mesmo. Findo o prazo de 3 (três) dias úteis, sem a resolução do problema, deverá a CONTRATADA disponibilizar em até 24 horas equipamento de especificação igual ou superior para operação temporária como substituição do equipamento em conserto, o qual deverá ser avaliada e autorizado por representante do Departamento de Informática, não ultrapassando o prazo máximo de 30 (trinta) dias para a solução definitiva do problema;
- 4.29.** O serviço de garantia será prestado com vistas a manter os equipamentos fornecidos em perfeitas condições de uso, sem qualquer ônus adicional para o Ministério Público do Estado do Pará. Nesse sentido, a garantia deve englobar:
- a)** A remoção dos vícios apresentados pelos equipamentos, materiais, drivers e outros componentes que sejam disponibilizados pelo fabricante dos equipamentos;
 - b)** Solução de problemas e esclarecimento de dúvidas de configuração e de utilização dos equipamentos;
- 4.30.** Os serviços deverão ocorrer de acordo com instruções a serem dadas pelo Departamento de Informática ou por servidor designado para esse fim. A realização dos serviços previstos, a serem efetuados nas dependências do Ministério Público do Estado do Pará, por funcionário da CONTRATADA, deverá ser acompanhada por profissional designado pelo Departamento de Informática do Ministério Público do Estado do Pará;
- 4.31.** As atividades de prestação de serviços de garantia aos equipamentos deverão ocorrer em dias úteis, no período de 8 (oito) às 14 (quatorze) horas;
- 4.32.** Durante todo o período da prestação de serviços de suporte técnico, a CONTRATADA deverá fornecer ao Contratante um usuário e senha para acesso ao sítio do Fabricante na Internet, onde deverá ser possível acompanhar o licenciamento instalado e, em área própria para o modelo ofertado, recursos para consulta e download de:
- 4.32.1.** Softwares, drivers e firmwares (atualizações e/ou versões completas);
 - 4.32.2.** Manuais de usuário e dos equipamentos;
 - 4.32.3.** Banco de solução para suporte ao software e hardware instalados de fábrica.
- 4.33.** A CONTRATADA deverá manter controle dos chamados abertos, registrando durante toda a vigência contratual ao menos as seguintes informações: número do chamado, número de série do equipamento, data de abertura do chamado, responsável pela abertura do chamado no MPPA, descrição do chamado, local da prestação dos serviços, peças substituídas, data de fechamento do chamado e responsável pela aprovação do fechamento do chamado no MPPA;
- 4.34.** A CONTRATADA deverá indicar, quando da assinatura do ARP/contrato, a empresa que prestará os serviços de garantia, com todas as informações necessárias (endereço completo, telefone, fax, e-mail e, se houver, responsável técnico) através de declaração assinada pelo representante legal da mesma, específica para este pregão. A substituição da empresa indicada para a prestação da garantia on-site somente poderá ser feita mediante comunicação e autorização prévia do Ministério Público do Estado do Pará;
- 4.35.** Durante o período da prestação de serviços de garantia e suporte técnico, devem ser disponibilizados e instalados, sem ônus à Contratante, todas as atualizações de software e firmware para os equipamentos, quando for necessário;
- 4.36.** Todos os equipamentos deverão ser previamente registrados pelo fornecedor junto ao fabricante, em nome da Contratante, caso seja uma exigência para fins de garantia;
- 4.37.** Substituir qualquer equipamento durante o prazo de suporte se, em um período de 6 (seis) meses, ocorrer mais de 3 (três) chamados referentes ao mesmo problema (desde que a causa-raiz do mesmo

tenha sido atribuída ao equipamento), ou mais de 5 (cinco) chamados referentes a problemas distintos (desde que a causa-raiz dos mesmos tenha sido atribuída ao equipamento);

4.38. A CONTRATADA deve fornecer opção de abertura de ocorrências através de sistema via WEB e através de telefone. O sistema via web, deve ser protegido por senha, permitir a abertura de ocorrências, geração automática do número da ocorrência e o envio automático de correio eletrônico (e-mails) para o pessoal envolvido. Os atendimentos referentes à instalação, análise de performance e ajuste de configurações serão realizados mediante agendamento prévio entre o pessoal técnico responsável da CONTRATANTE e da CONTRATADA. Ao término de cada atendimento a CONTRATADA deve gerar relatório descrevendo as atividades realizadas e o tempo gasto para tal, este relatório deve ser aprovado pela CONTRATADA.

4.39. Quando da assinatura do contrato, comprovar **através de documentação do fabricante** que os equipamentos especificados para os itens 01 a 03 são novos e de primeiro uso, e que não estarão fora da linha de produção nos próximos **120 (cento e vinte) dias** após a entrega dos mesmos;

4.40. Caso os produtos entregues não sejam de fabricação nacional, deverá ser apresentada original ou cópia autenticada da Declaração de Importação, emitida pela Receita Federal;

4.41. Relativamente, ao disposto nesta cláusula, aplicam-se também, subsidiariamente, no que couber, as disposições da Lei nº 8.078 de 11/09/90 – Código de Defesa do Consumidor;

4.42. Entrega dos Serviços de Instalação/Configuração:

4.42.1. O serviço de Instalação/Configuração deve ser executado no máximo após 30 dias da entrega dos equipamentos;

4.42.2. O Serviço de Instalação/Configuração será dado como entregue com o atendimento de todos os itens e subitens descritos no tópico 3.32.5. “Item 05 - Serviço de Instalação/Configuração”;

4.42.3. Entrega do plano de implantação atualizado, aprovado pela equipe técnica do MPPA com o descritivo de todos os serviços que foram executados, contendo topologia física, lógica e endereçamento implementado;

4.42.4. Instalação física e configuração de todos os equipamentos adquiridos no local determinado pela equipe de TI no anexo II, conforme plano de implantação com todas as atualizações e configurações do sistema de Firewall, SD-WAN, VPN, IPS, Filtro URL, Antivírus e Anti-Malware de acordo com os requisitos levantados;

4.42.5. A migração de todas as regras de Firewall, VPN, IPS, Filtro URL, Antivírus e Anti-Malware do dispositivo antigo para o novo firewall;

4.42.6. Entrega do relatório de instalação e configuração, contendo toda documentação das instalações e configurações efetuadas, as decisões tomadas, diagramas e topologias em formato legível e tecnicamente fundamentado;

4.42.7. Aceite do **item** Instalação/Configuração pelo fiscal ou suplente do contrato.

4.43. Entrega do Serviço Treinamento:

4.43.1. A entrega do serviço deve atender todos os itens descritos no tópico 3.32.6. Item 06 - Treinamento “Hands On” sobre Solução de Firewall/SD-WAN;

4.43.2. O serviço denominado Treinamento deve ser iniciado no primeiro dia útil após a conclusão do serviço de Instalação/Configuração e finalizado no prazo máximo de 15 dias corridos a contar da conclusão da instalação/configuração dos equipamentos;

4.43.3. O treinamento deve ser ministrado em língua portuguesa e deve ser realizado com material didático em PDF, elaborado pelo fabricante ou CONTRATADA;

4.43.4. A parte prática deve ser executada, nas dependências do Ministério Público, que fornecerá, à equipe própria de trabalho, computadores e acesso à internet para desenvolvimento das atividades em ambiente de teste virtual ou on-line disponibilizado pelo fabricante ou pela contratada por este homologado;

4.43.5. A CONTRATADA deve informar com antecedência mínima de 05 dias úteis, requisitos específicos para realização do treinamento, tais como: acesso a domínios, protocolos, portas, serviços, ips, dentre outros;

4.43.6. O treinamento deve ser do tipo “hands on training”, com foco prático na implantação, configuração básica e avançada, troubleshoot, monitoramento e gerencia da solução de Firewall/SD-WAN fornecida pela CONTRATADA, e também baseado no caso concreto das necessidades deste Parquet;

4.43.7. O certificado deve conter a carga horária do curso (20 horas) e ser entregue pela CONTRATADA até 05 dias após a conclusão do curso;

4.43.8. Ocasião em que será feita a conferência, pelo Departamento de Informática, da quantidade de horas ministradas e verificação da conformidade dos itens exigidos neste instrumento;

4.43.9. O não cumprimento dos prazos acima, sujeitará a CONTRATADA em mora, cujo atraso computar-se-á desde o primeiro dia do vencimento do prazo;

4.43.10. O serviço de Treinamento “Hands On” será considerado entregue após a conclusão de 20 horas aulas e entrega do certificado;

4.43.11. Na hipótese de ser verificada a impropriedade do treinamento ministrado, o mesmo será rejeitado, no todo ou em parte, a critério da FISCALIZAÇÃO responsável pelo seu recebimento, sendo o fornecedor obrigado a refazer o treinamento no prazo máximo de 15 (quinze) dias úteis após a verificação sem qualquer ônus para a Administração, independentemente da aplicação das penalidades cabíveis;

5 DIREITOS E OBRIGAÇÕES DO CONTRATANTE

5.1. Sem que a isto limite seus direitos, terá o Ministério Público as seguintes garantias:

5.1.1. Receber o objeto de acordo com o que consta neste instrumento, no edital e nos seus anexos;

5.1.2. Devolver o objeto em desacordo com as especificações exigidas no edital.

5.2. Sem que a isto limite sua responsabilidade, será o Órgão responsável pelos seguintes itens:

5.2.1. Cumprir e fazer cumprir o disposto nas condições deste Termo de Referência;

5.2.2. Cumprir todos os compromissos financeiros assumidos com a CONTRATADA no prazo estipulado;

5.2.3. Proporcionar todas as facilidades, inclusive esclarecimentos atinentes ao objeto, para que a empresa possa cumprir as obrigações dentro das normas e condições da aquisição;

5.2.4. Indicar servidor com competência necessária para proceder o recebimento dos objetos licitados e atestar as Notas Fiscais após a verificação das especificações, qualidade, quantidade e preços pactuados;

5.2.5. Promover, através de seu representante, o acompanhamento e a fiscalização do objeto contratado, sob os aspectos quantitativos e qualitativos, prazos de vigência e entregas, anotando em registro próprio as falhas detectadas e comunicando ao Órgão por escrito as advertências e as ocorrências de quaisquer fatos que, a seu critério, exijam medidas corretivas por parte desta;

5.2.6. Solicitar, mediante pedido de fornecimento, a quantidade necessária ao seu uso regular, observada a estimativa constante no Termo de Referência;

5.2.7. Emitir nota de empenho a crédito do fornecedor no valor correspondente à quantidade solicitada;

5.2.8. Acompanhar e fiscalizar a perfeita execução do CONTRATO;

5.2.9. Efetuar o pagamento à CONTRATADA referente à quantia efetivamente entregue e após o cumprimento das formalidades legais, no prazo máximo de 30 (trinta) dias corridos contados do atesto da respectiva nota fiscal do material entregue.

6 DIREITOS E OBRIGAÇÕES DO CONTRATADO

6.1. Sem que a isto limite suas garantias, a CONTRATADA terá os seguintes direitos:

6.1.1. Receber informações e esclarecimentos necessários ao cumprimento das condições estabelecidas;

6.1.2. Receber o Atesto do recebimento do objeto contratado após verificação das especificações;

6.1.3. Receber formalmente a notificação de ocorrência de irregularidades que a fiscalização identificar na execução do objeto licitado, até para que possa a empresa proceder correções;

6.1.4. Receber o pagamento nas condições estabelecidas neste instrumento.

6.2. Sem que a isto limite sua responsabilidade, será a CONTRATADA responsável pelos seguintes itens:

6.2.1. Cumprir fielmente as obrigações assumidas, conforme as especificações no Edital e no Termo de Referência, zelando pela fiel execução, utilizando-se de todos os recursos materiais e humanos necessários;

6.2.2. Fornecer o objeto adjudicado para o qual se sagrar vencedora, em estrita conformidade com as especificações e condições exigidas neste Termo e na licitação pertinente, bem como naquelas resultantes de sua proposta, devendo já estar inclusos nos valores propostos todos os custos, impostos, taxas e demais encargos pertinentes à formação do preço;

- 6.2.3.** Atender todos os pedidos de fornecimento efetuados pelo CONTRATANTE durante a vigência da Ata, mesmo que a entrega deles decorrentes esteja prevista para data posterior ao seu vencimento;
- 6.2.4.** Entregar os equipamentos e manuais e os prospectos em português no prazo, local e horário previstos no Termo de Referência e ARP/ Contrato, observando rigorosamente as exigências estabelecidas nas especificações e na proposta de preços apresentada pela empresa;
- 6.2.5.** Durante o recebimento, substituir o equipamento não aceito pela Contratante em prazo não superior a 30 (trinta) dias corridos, contados da ciência da rejeição;
- 6.2.6.** Responsabilizar-se pelo ônus de retirada e devolução dos equipamentos para realização de serviços de suporte técnico fora das dependências da Contratante;
- 6.2.7.** A CONTRATADA é obrigada a reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, o objeto desta licitação em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou de materiais empregados;
- 6.2.8.** Arcar com todas as despesas, diretas ou indiretas, decorrentes do cumprimento das obrigações assumidas, responsabilizando-se pelos danos causados diretamente à administração ou a terceiros, decorrentes de sua culpa ou dolo, por ocasião da entrega dos objetos licitados no local indicado, incluindo os possíveis danos causados por transportadoras, sem qualquer ônus ao contratante.
- 6.2.9.** Ser responsável pelos encargos trabalhistas, previdenciários, fiscais e comerciais resultantes da execução; a inadimplência da licitante, com referência aos encargos estabelecidos neste item não transfere a responsabilidade por seu pagamento à Administração do Ministério Público, nem poderá onerar o objeto desta licitação, razão pela qual a CONTRATADA renuncia expressamente a qualquer vínculo de solidariedade, ativa ou passiva, com o Ministério Público;
- 6.2.10.** Quando da assinatura do contrato, comprovar através de documentação do fabricante que os equipamentos especificados para os itens 01 a 03 são novos e de primeiro uso, e que não estarão fora da linha de produção nos próximos 120 (cento e vinte) dias após a entrega dos mesmos;
- 6.2.11.** Caso os produtos entregues não sejam de fabricação nacional, deverá ser apresentada original ou cópia autenticada da Declaração de Importação, emitida pela Receita Federal;
- 6.2.12.** Prestar todos os esclarecimentos que forem solicitados pelo Ministério Público, durante o prazo de fornecimento, credenciando, junto ao Órgão, um representante para prestar os devidos esclarecimentos e atender as reclamações que porventura surgirem durante a execução;
- 6.2.13.** Manter durante todo o prazo de vigência da relação obrigacional com a Contratante a regularidade com o fisco, com o sistema de seguridade social, com a legislação trabalhista, normas e padrões de proteção ao meio ambiente e cumprimento dos direitos da mulher, inclusive os que protegem a maternidade, sob pena da rescisão contratual, sem direito a indenização conforme preceitua o art. 28, §4º da Constituição do Estado do Pará, assim como todas as leis e posturas federais, estaduais e municipais, vigentes, sendo a única responsável por prejuízos decorrentes de infrações a que houver dado causa.
- 6.2.14.** Quando, por problemas, técnicos os prazos pactuados não puderem ser cumpridos, a CONTRATADA deverá comunicar por escrito ao Órgão até 02 (dois) dias úteis anteriores ao término do prazo, ao qual caberá aceitar ou rejeitar as justificativas;
- 6.2.15.** Manter, durante toda a execução, todas as condições de habilitação e qualificação exigidas no Pregão que sejam compatíveis com as obrigações a serem assumidas:
- 6.2.15.1.** Regularidade Fiscal com a Fazenda Nacional, o Sistema de Seguridade Social e o Fundo de Garantia do Tempo de Serviço – FGTS;
 - 6.2.15.2.** Regularidade Fiscal perante as Fazendas Estaduais e Municipais da sede da licitante;
 - 6.2.15.3.** Regularidade Trabalhista;
 - 6.2.15.4.** Cumprimento do disposto no art. 7º, XXXIII, da Constituição Federal/88 (trabalho de menores de idade, observada a Lei nº 9.854/1999);
- 6.2.16.** Informar o Órgão de qualquer alteração necessária à consolidação dos ajustes decorrentes da execução do objeto, tais como: mudança de endereço, razão social, telefone, fax, dissolução da sociedade, falência e outros;
- 6.2.17.** Assumir inteira responsabilidade técnica e administrativa do objeto ADJUDICADO, não podendo, sob qualquer hipótese, transferir a outras empresas a responsabilidade por problemas de funcionamento;
- 6.2.18.** Respeitar e obedecer às normas fixadas pela Administração da CONTRATANTE;
- 6.2.19.** O inadimplemento das obrigações da CONTRATADA, com referência aos encargos trabalhistas, previdenciários, fiscais e comerciais, resultantes da execução da ARP, não transfere à

Administração da CONTRATANTE a responsabilidade por seu pagamento, nem pode onerar o objeto deste Termo de Referência;

6.2.20. Não transferir a outrem, no todo ou em parte, o objeto do presente, sem prévia e expressa anuência do Ministério Público;

6.2.21. A CONTRATADA é obrigada a reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, o objeto desta licitação em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou de materiais empregados.

6.2.22. Responder por acidentes de que possam ser vítimas seus profissionais e, ainda, por eventuais danos causados no local entrega do objeto, aos servidores da CONTRATANTE, bem como a terceiros, quando praticados, por dolo, negligência, imperícia ou imprudência, diretamente por seus empregados na execução do ajuste, arcando, após regular processo administrativo, com a restauração, substituição ou indenização, conforme o caso, devendo os funcionários da empresa contratada apresentarem documentos (RG e CPF) para que seja providenciada a autorização de acesso aos locais indicados na nota de empenho;

6.2.23. Comunicar imediatamente à Administração, bem como ao responsável pela fiscalização, qualquer anormalidade verificada, inclusive de ordem funcional, para que sejam adotadas as providências de regularização necessárias, em qualquer tempo até o final da garantia;

6.2.24. Quando da prestação do eventual serviço de garantia ao equipamento:

6.2.24.1. Fazer-se representar, no local da prestação do eventual serviço de Garantia, por preposto aceito pela Administração com a atribuição de coordenar e fiscalizar a execução dos serviços e o cumprimento das normas disciplinares, de segurança e legislação pertinentes;

6.2.24.2. Atender prontamente às chamadas e às determinações do representante da Administração da CONTRATANTE com vistas a corrigir defeitos observados nos equipamentos entregues dentro do prazo de garantia;

6.2.24.3. Utilizar pessoal técnico qualificado, devidamente identificado com crachás contendo nome, foto e cargo/função desempenhada nas dependências da CONTRATANTE;

6.2.24.4. Comprovar, quando solicitado, a qualificação técnica dos funcionários que irão atender o MPPA;

6.2.24.5. Assumir a responsabilidade por todas as providências e obrigações estabelecidas na legislação específica de acidentes do trabalho, quando, em ocorrência da espécie, forem vítimas os seus empregados no desempenho dos serviços de Assistência Técnica ou em conexão com eles, ainda que acontecido nas dependências da CONTRATANTE;

6.2.25. Assumir todos os encargos sobre demanda trabalhista, previdenciários, obrigações sociais previstas na legislação social e trabalhista em vigor, cível ou penal, relacionado ao eventual serviço de Garantia, originariamente ou vinculados por prevenção, conexão ou contingência, além de assumir a responsabilidade pelos encargos fiscais e comerciais;

6.2.26. São de responsabilidade da CONTRATADA todas e quaisquer despesas decorrentes de sua atividade;

6.2.27. Observar a Resolução nº 172/2017-CNMP que altera o artigo 3º, caput, da Resolução CNMP nº 37/2009 e VEDA ao Ministério Público a contratação das pessoas jurídicas que tenham em seu quadro societário cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade até o terceiro grau, inclusive, dos membros ocupantes de cargos de direção ou no exercício de funções administrativas, assim como de servidores ocupantes de cargos de direção, chefia e assessoramento vinculados direta ou indiretamente às unidades situadas na linha hierárquica da área encarregada da licitação;

6.2.27.1. A vedação do item 6.2.27 não se aplica às hipóteses nas quais a contratação seja realizada por ramo do Ministério Público diverso daquele ao qual pertence o membro ou servidor gerador da incompatibilidade.

6.2.27.2. A vedação do item 6.2.27 se estende às contratações cujo procedimento licitatório tenha sido deflagrado quando os membros e servidores geradores de incompatibilidade estavam no exercício dos respectivos cargos e funções, assim como às licitações iniciadas até 6 (seis) meses após a desincompatibilização.

6.2.27.3. A contratação de empresa pertencente a parente de membro ou servidor não abrangido pelas hipóteses expressas de nepotismo poderá ser vedada pelo órgão do Ministério Público competente, quando, no caso concreto, identificar risco potencial de contaminação do processo licitatório.

6.2.28. Aceitar o fato de que as informações obtidas em decorrência da execução do presente Termo deverão ser mantidas em sigilo, não podendo qualquer participante divulgá-las fora do âmbito deste instrumento, exceto se previamente acordado por escrito, ou prevista a sua divulgação.

6.2.29. Observar a VEDAÇÃO de contratação de Empresa que tenha entre seus empregados colocados à disposição do Ministério Público para o exercício de funções de chefia, pessoas que incidam na vedação dos arts. 1º e 2º da **Resolução nº 177/2017-CNMP:**

6.2.29.1. Pessoa que tenha sido condenada em decisão com trânsito em julgado ou proferida por órgão jurisdicional colegiado, nos seguintes casos:

- I – atos de improbidade administrativa;
- II – crimes:
 - a) contra a administração pública;
 - b) contra a incolumidade pública;
 - c) contra a fé pública;
 - d) contra o patrimônio;
 - e) de abuso de autoridade, nos casos em que houver condenação à perda do cargo ou à inabilitação para o exercício de função pública;
 - f) de tráfico de entorpecentes e drogas afins, racismo, tortura, terrorismo e hediondos;
 - g) contra a vida e a dignidade sexual;
 - h) praticados por organização ou associação criminosa;
 - i) de redução de pessoa à condição análoga à de escravo;
 - j) eleitorais, para os quais a lei comine pena privativa de liberdade;
 - k) de lavagem ou ocultação de bens, direitos e valores.

6.2.29.2. Aqueles que tenham:

- I – praticado atos causadores da perda do cargo ou emprego público, reconhecidos por decisão transitada em julgado ou proferida por órgão judicial colegiado;
- II – sido excluídos do exercício da profissão, por decisão definitiva sancionatória judicial ou administrativa do órgão profissional competente, salvo se o ato houver sido anulado ou suspenso pelo Poder Judiciário;
- III – tido suas contas relativas ao exercício de cargos ou funções públicas rejeitadas por irregularidade insanável que configure ato doloso de improbidade administrativa, por decisão irreversível do órgão competente, salvo se esta houver sido suspensa ou anulada pelo Poder Judiciário, devendo tal condição constar expressamente dos editais de licitação.

7 PRAZO E CONDIÇÕES DE PAGAMENTO

7.1. O pagamento será efetuado pelo Departamento Financeiro do Ministério Público no prazo máximo de **30 (trinta) dias** corridos, no Banco: xxxxxx, Agência nº xxxxx, Conta Corrente nº xxxx, salvo atraso na liberação de recursos pela Secretaria Executiva de Planejamento, Orçamento e Finanças - SEPOF, após o recebimento definitivo **da solução e dos serviços licitados**, mediante a apresentação **das Notas Fiscais devidamente atestadas** pelo FISCAL, o qual observará as especificações exigidas no Edital e no Termo de Referência.

7.1.1. O pagamento dos fornecedores de bens e prestadores de serviços dos órgãos da Administração Direta e Indireta do Estado do Pará será efetuado mediante crédito em conta corrente aberta no Banco do Estado do Pará S/A – BANPARÁ, conforme Decreto Estadual nº 877, de 31/03/2008.

7.1.2. Caso o prestador não possua conta no banco BANPARÁ, será cobrada pelo banco taxa referente ao DOC/TED, sendo o valor desta taxa automaticamente descontado no valor depositado para pagamento da prestação do serviço.

7.1.3. Pagamentos através de código de barra só poderão ser realizados caso a empresa possua convênio com o Banco do Estado do Pará (BANPARÁ), uma vez que todos os pagamentos são realizados através do SIAFEM (Sistema Integrado de Administração Financeira de Estados e Municípios).

7.2. O atesto da nota fiscal será efetuado no prazo máximo de 05 (cinco) dias úteis contados do recebimento definitivo do material pelo responsável pela Fiscalização no local anteriormente mencionado;

7.3. A nota fiscal que contiver erro será devolvida à contratada para retificação e reapresentação, iniciando a contagem dos prazos fixados para o ATESTO a partir do recebimento da Nota Fiscal corrigida.

- 7.4. A CONTRATADA deverá encaminhar, junto com a nota fiscal, os seguintes documentos:
- 7.4.1. Certidão conjunta negativa de débitos relativos aos tributos federais e a dívida ativa da União;
 - 7.4.2. Certidão negativa de débitos relativos às Contribuições Previdenciárias;
 - 7.4.3. Certificado de regularidade do FGTS – CRF;
 - 7.4.4. Certidão negativa de débitos inadimplidos perante a Justiça do Trabalho;
 - 7.4.5. Certidão negativa de débitos com Fazenda Estadual;
 - 7.4.6. Certidão negativa de débitos com a Fazenda Municipal;
- 7.5. Ocorrendo erro no documento da cobrança, este será devolvido e o pagamento será susgado para que a CONTRATADA tome medidas necessárias, passando o prazo para o pagamento a ser contado a partir da data da reapresentação do mesmo.

8 ACOMPANHAMENTO DA EXECUÇÃO

- 8.1. A execução das atividades contratuais, em conformidade com as disposições contidas no inciso III do art. 58 c/c o art. 67 da Lei nº 8.666/93, será acompanhada e fiscalizada por servidor especificamente designado, competindo-lhe, dentre outras atividades:
- 8.1.1. Fiscalizar a execução do presente contrato, de modo a que sejam cumpridas, integralmente, as condições constantes de suas cláusulas;
 - 8.1.2. Comprovar e relatar por escrito as eventuais irregularidades;
 - 8.1.3. Determinar o que for necessário à regularização de faltas ou defeitos verificados, podendo sustar a execução de quaisquer trabalhos, em casos de desacordo com o especificado ou por motivo que caracterize a necessidade de tal medida;
 - 8.1.4. Sugerir que seja susgado o pagamento das faturas, no caso de inobservância pela CONTRATADA das suas obrigações constantes do presente contrato;
- 8.2. O acompanhamento e a fiscalização da execução do contrato consistem na verificação da conformidade da execução do objeto e da alocação dos recursos necessários, de forma a assegurar o perfeito cumprimento do contrato;
- 8.3. A fiscalização exercida pela Contratante não excluirá ou reduzirá a responsabilidade da CONTRATADA pela completa e perfeita execução do objeto contratual, tampouco restringe a responsabilidade integral e exclusiva da CONTRATADA quanto à integralidade e à correção dos fornecimentos a que se obrigou, suas consequências e implicações perante terceiros, próximas ou remotas;
- 8.4. A CONTRATADA declara aceitar, integralmente, todos os métodos e processos de inspeção, verificação e controle a serem adotados pela Contratante.

9 PENALIDADES

No caso de não cumprimento das obrigações oriundas deste instrumento, serão cominadas as seguintes penalidades:

9.1. ADVERTÊNCIA

Advertência pelo não cumprimento de obrigações assumidas, desde que não interfira na execução dos compromissos assumidos ou na sua conclusão e não traga sérios prejuízos econômicos e funcionais a este Órgão;

9.2. MULTA

9.2.1. De 0,25% ao dia, até o limite máximo de 5%, sobre o valor total **do Lote adjudicado**, nos casos de atraso injustificado nos prazos de **assinatura da ata de registro de preços**.

9.2.1.1. Após o 20º dia de atraso dos prazos previstos, sem justificativa aceita pela Administração, o objeto será considerado como inexecutado.

9.2.2. De 0,25% ao dia, até o limite máximo de 5%, sobre o valor total **do item solicitado**, nos casos de atraso injustificado nos prazos de **assinatura do Contrato; retirada/aceite da nota de empenho**.

9.2.2.1. Após o 20º dia de atraso dos prazos previstos, sem justificativa aceita pela Administração, o objeto será considerado como inexecutado.

9.2.3. De 0,25% ao dia, até o limite máximo de 5%, sobre o valor total **da respectiva nota de empenho**, nos casos de atraso injustificado nos prazos **entrega do objeto; substituição do objeto**.

9.2.1.1. Após o 20º dia de atraso dos prazos previstos, sem justificativa aceita pela Administração, o objeto será considerado como inexecutado.

9.2.4. De **10%**, sobre o valor total **do Lote adjudicado**, nos casos de recusa injustificada em assinar a **Ata de Registro de Preços**, se configurar inexecução total;

9.2.5. De **10%**, sobre o valor total **do item solicitado**, nos casos de:

- I. Recusa injustificada em assinar o **Contrato**, se configurar inexecução total
- II. Recusa injustificada em retirar/aceitar a **nota de empenho**, se configurar inexecução total;

9.2.6. De **10%**, sobre o valor total **da respectiva nota de empenho**, nos casos de:

- I. Recusa injustificada em **entregar/executar o objeto**, se configurar inexecução total;
- II. Recusa injustificada em substituir o objeto recusado ou com vícios, se configurar inexecução total;
- III. Outras hipóteses de inexecução total do objeto.

9.2.7. De 10%, sobre o valor total **da respectiva nota de empenho**, nos casos de:

- I. Recusa injustificada em retirar/aceitar a nota de empenho, se configurar inexecução parcial;
- II. Entregar/executar parcial o objeto;
- III. Recusa injustificada em substituir o objeto recusado ou com vícios, se configurar inexecução parcial;
- IV. Outras hipóteses de inexecução parcial do objeto.

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

9.2.8. De 5% sobre o valor total **da respectiva nota de empenho** nos casos de irregularidade no cumprimento do objeto ou na prestação da garantia do produto do objeto contratado, não referidas nos itens anteriores

9.2.7. As multas são autônomas e a aplicação de uma não exclui a outra;

9.2.8. Havendo garantia à execução apresentada pela empresa, o valor da multa será descontado da mesma. Não havendo garantia ou caso o valor da multa seja superior à referida, a multa ou a diferença será cobrada administrativamente pela Contratante, podendo ser descontado dos créditos devidos, ou ainda judicialmente.

9.3. SUSPENSÃO

9.3.1. Nos casos de inexecução total ou parcial do objeto ou irregularidades na execução, não justificada e/ou não aceita pela Administração desde que não incluída como hipótese do item 28.4.1 do edital, aplicar-se-á Suspensão Temporária de participar em licitação e impedimento de contratar com o Ministério Público do Estado do Pará, pelo período de até 02 (dois) anos, na seguinte graduação:

- I. 1 (um) ano, nos casos de inexecução parcial ou irregularidades na execução do objeto;
- II. 2 (dois) anos, nos casos de inexecução total.

9.4. DECLARAÇÃO DE INIDONEIDADE

9.4.1. No caso de inexecução do objeto que configure ilícito penal, será declarada a inidoneidade da Contratada para licitar e contratar com a Administração Pública Estadual, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade.

10. DISPOSIÇÕES GERAIS/INFORMAÇÕES COMPLEMENTARES

10.1.1. As licitantes, antes de apresentarem suas propostas, devem analisar toda a documentação referente a presente licitação, dirimindo, oportunamente, todas as dúvidas, de modo a não

incorrerem em missões que jamais poderão ser alegadas em favor de eventuais pretensões de acréscimo dos preços propostos.

Belém, 07 de outubro de 2019.

Regivaldo N. Lopes Pereira
Analista de Sistemas – Suporte a Rede de Computadores

ADRIANO SILVA DE ARRUDA
Diretor do Departamento de Informática

ANEXO I – DO TR (TERMO DE REFERÊNCIA)

1. LOCALIDADES

Item do edital:

Unidade. Endereço. Telefone.

Item 1 (NGFW de pequeno porte):

Núcleo de Atendimento Integrado (NAI). Avenida Governador José Malcher, 1031, Bloco B, 3º andar - Nazaré, Belém –PA, 66055-260. (91) 3272-2400;

Item 1 (NGFW de pequeno porte):

Promotoria de Justiça de Defesa do Cidadão e da Comunidade. Av. Doutor Freitas, 2513 - Marco, Belém - PA, 66087-810. (91) 3182-2307, (91) 3182-2305, (91) 3182-2318;

Item 2 (NGFW de médio porte):

Promotoria de Justiça de Icoaraci. Rua Manoel Barata, 1289 - Cruzeiro (Icoaraci), Belém – PA, 66810-971. (91) 3218-7700, (91) 3218-7703, (91) 3218-7704;

Contato Setor de Redes: (91)4006-3412, (91)4006-3644, (91)4006-3974, (91)4006-3545

Horários de funcionamento das unidades: das 08:00-14:00.

ANEXO II

MINUTA ATA DE REGISTRO DE PREÇOS Nº XXX/2021-MP/PA

O **MINISTÉRIO PÚBLICO DO ESTADO DO PARÁ**, pessoa jurídica de direito público interno, inscrita no CNPJ/MF sob o n.º 05.054.960/0001-58, estabelecida nesta capital à Rua João Diogo, 100, bairro Cidade Velha, CEP: 66015-165, neste ato representada pelo Exmo. Sr. Dr....., brasileiro, residente nesta Capital, doravante denominado(a) **ADMINISTRAÇÃO** e a Empresa, pessoa jurídica de direito privado, inscrita no CNPJ/MF sob n.º, Inscrição Estadual n.º, com sede na, neste ato representada pelo Sr(a) (nacionalidade, estado civil, profissão), portador(a) do RG n.º e do CPF/MF n.º, residente e domiciliado(a), na, na cidade de, doravante denominada **COMPROMITENTE FORNECEDOR**, resolvem firmar a presente ATA DE REGISTRO DE PREÇOS, de acordo com o resultado do Pregão Eletrônico n.º 047/2020-MP/PA, mediante as cláusulas e condições a seguir estabelecidas e com fundamento no Decreto Estadual 991, de 24 de agosto de 2020:

CLÁUSULA PRIMEIRA - DO OBJETO

O presente termo tem por objeto e finalidade o **Registro de Preços para aquisição de ativos de segurança de rede, Firewalls Next Generation (NGFW) com SD-WAN integrada, contemplando os serviços de Instalação, Treinamento e Suporte Técnico**, nas condições definidas no ato convocatório, seus anexos, propostas de preços e ata do Pregão Eletrônico Nº 047/2020-MP/PA vinculada ao **PROCESSO Nº. 162/2019-SGJ-TA (PROTOCOLO Nº 45212/2019)** que integram este instrumento independente de transcrição, pelo prazo de validade do registro.

CLÁUSULA SEGUNDA - DO PREÇO

2.1 O(s) preço(s) registrado(s), a quantidade, o(s) fornecedor(es) e as especificações dos objetos constantes deste instrumento encontram-se contidos na tabela abaixo, obedecida a ordem de classificação:

2.1.1 O valor global estimado desta Ata é de R\$

2.2 O preço registrado já inclui todas as despesas necessárias, sem quaisquer ônus para o **MINISTÉRIO PÚBLICO** no que se refere a frete, tributos e outros.

2.3 Com objetivo de formação de cadastro de reserva, no caso de impossibilidade de atendimento pelo primeiro colocado da ata nas hipóteses previstas nos arts. 22 e 23 do **Decreto Estadual 991, de 24 de agosto de 2020**, ficará registrado na Ata de Formação de Cadastro de Reserva (Anexo I desta ARP) do pregão os licitantes aptos e/ou que aceitaram cotar os bens com preços iguais ao do licitante vencedor na sequência da classificação do certame, devendo a ordem de classificação ser respeitada nas contratações.

- I. 2º Classificada – Nome e CNPJ;
- II. 3º Classificada – Nome e CNPJ;
- III. 4º Classificada – Nome e CNPJ;

CLÁUSULA TERCEIRA - DA RENEGOCIAÇÃO DE PREÇOS

3.1.. Os preços registrados poderão ser revistos em decorrência de eventual redução dos preços praticados no mercado ou de fato que eleve o custo dos serviços ou bens registrados, cabendo ao órgão gerenciador promover as negociações junto aos fornecedores, observadas as disposições contidas na alínea "d", do inciso II do caput do art. 65 da lei nº 8.666, de 21 de junho de 1993.

3.1 Quando o preço registrado tornar-se superior ao preço praticado no mercado por motivo superveniente, o órgão gerenciador convocará os fornecedores para negociarem a redução dos preços aos valores praticados pelo mercado.

3.1.1 Os fornecedores que não aceitarem reduzir seus preços aos valores praticados pelo mercado serão liberados do compromisso assumido, sem aplicação de penalidade.

3.1.2 A ordem de classificação dos fornecedores que aceitarem reduzir seus preços aos valores de mercado observará a classificação original.

3.2 Quando o preço de mercado tornar-se superior aos preços registrados e o fornecedor não puder cumprir o compromisso, o órgão gerenciador poderá:

- I. Liberar o fornecedor do compromisso assumido, caso a comunicação ocorra antes do pedido de fornecimento, e sem aplicação da penalidade se confirmada a veracidade dos motivos e comprovantes apresentados;
- II. Convocar os demais fornecedores para assegurar igual oportunidade de negociação.

3.2.1 Não havendo êxito nas negociações, o órgão gerenciador deverá proceder à revogação da Ata de Registro de Preços, adotando as medidas cabíveis para obtenção da contratação mais vantajosa.

CLÁUSULA QUARTA - DO CANCELAMENTO DOS PREÇOS REGISTRADOS

4.1. O registro do fornecedor será cancelado quando:

- I. Descumprir as condições da Ata de Registro de Preços;
- II. Não retirar a nota de empenho ou instrumento equivalente no prazo estabelecido pela Administração, sem justificativa aceitável;
- III. Não aceitar reduzir o seu preço registrado, na hipótese deste se tornar superior àqueles praticados no mercado; ou
- IV. Sofrer sanção prevista nos incisos III ou IV do caput do art. 87 da lei nº 8.666, de 21 de junho de 1993, ou no art. 7º da lei nº 10.520, de 17 de julho de 2002.

4.1.1. O cancelamento de registros nas hipóteses previstas nos incisos I, II e IV do caput será formalizado por despacho do órgão gerenciador, assegurado o contraditório e a ampla defesa.

4.2. O cancelamento do registro de preços poderá ocorrer por fato superveniente, decorrente de caso fortuito ou força maior, que prejudique o cumprimento da Ata, devidamente comprovado e justificado:

- I. Por razão de interesse público; ou
- II. A pedido do fornecedor.

CLÁUSULA QUINTA – DOS PEDIDOS

5.1. O MINISTÉRIO PÚBLICO solicitará, mediante Nota de Empenho e/ou Contrato, a quantidade necessária ao seu consumo regular, observada a estimativa, não havendo impedimento que a quantidade e período regular de fornecimento sejam modificados em razão da necessidade do órgão, devidamente justificada;

5.2. O registro dos preços efetivados na Ata não obriga a Administração a firmar contratações que deles poderão advir, cabendo, contudo, na hipótese de opção por outro meio de contratação, assegurar ao beneficiário do registro preferência em igualdade de condições.

5.3. Os detentores da Ata de Registro de Preços ficam obrigados a atender todos os pedidos de fornecimento efetuados pelo ÓRGÃO durante a vigência da Ata, mesmo que a entrega deles decorrentes esteja prevista para data posterior ao seu vencimento.

CLÁUSULA SEXTA - DA UTILIZAÇÃO DA ATA DE REGISTRO DE PREÇOS POR ÓRGÃO OU ENTIDADES NÃO PARTICIPANTES

6.1. Considerando a discricionariedade administrativa e diante da previsão expressa no artigo 24 do **Decreto Estadual 991, de 24 de agosto de 2020**, os órgãos não participantes poderão utilizar a ata de registro de preços decorrente deste certame, mediante a devida solicitação de adesão;

6.1.1. Não poderão aderir os órgãos da administração pública federal, nos termos do Decreto Federal nº 7.892/2013;

6.1.2. O deferimento de adesão será submetido à avaliação de sua conveniência e ausência de prejuízo para as demandas do Ministério Público.

6.2. As adesões à Ata, se autorizadas pela Administração do Ministério Público, serão regidas pelo **Artigo 22 do Decreto Federal nº 7.892/2013**, e não poderão exceder, por órgão ou entidade, a **cinquenta** por cento dos quantitativos dos itens do instrumento convocatório e registrados na Ata de Registro de Preços para o órgão gerenciador;

6.3. 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 para o órgão gerenciador e órgãos participantes, independentemente do número de órgãos não participantes que aderirem, conforme item 30.3 do edital:

CLÁUSULA SÉTIMA – DA VIGÊNCIA

7.1. A vigência do presente instrumento será de 12 (doze) meses, improrrogáveis, contados da data da publicação deste instrumento no Diário Oficial do Estado do Pará.

CLÁUSULA OITAVA - DAS SUPRESSÕES

8.1. A supressão dos produtos registrados na Ata de Registro de Preço poderá ser total ou parcial, a critério do Órgão Gerenciador, considerando-se o disposto no §4º do Art. 15 da lei nº 8.666/93 e alterações.

CLÁUSULA NONA - DA DOTAÇÃO ORÇAMENTÁRIA

9.1. Os recursos financeiros para atender às despesas decorrentes desta licitação estão previstos na dotação orçamentária, sob a seguinte classificação funcional programática:

Classificação: 12101.03.122.1494.8760 – Governança e Gestão

Elemento: 4490-52 – Equipamentos e Material Permanente

Fonte: 0301 – Recursos Ordinários

Elemento: 3390-40 – Serviços da Tecnologia da Informação e Comunicação

Fonte: 0101 – Recursos Ordinários

CLÁUSULA DÉCIMA - DA EFICÁCIA

A presente Ata de Registro de Preços somente terá eficácia após a publicação do respectivo extrato no Diário Oficial do Estado.

CLÁUSULA DÉCIMA PRIMEIRA - DO FORO

Fica eleito o Foro da Justiça Estadual do Pará, Comarca de Belém-PA, para dirimir quaisquer questões oriundas do presente instrumento.

E, por estarem justas e compromissadas, as partes assinam o presente Termo em duas vias, de igual teor, na presença das testemunhas abaixo assinadas.

Belém-Pa, de de 2021

MINISTÉRIO PÚBLICO DO ESTADO DO PARÁ

COMPROMITENTE FORNECEDOR

Testemunhas:

RG: _____

RG: _____

ANEXO III

MINUTA CONTRATO Nº./2021-MP/PA

CONTRATO QUE ENTRE SI FAZEM O MINISTÉRIO PÚBLICO DO ESTADO DO PARÁ E A EMPRESA

.....

MINISTÉRIO PÚBLICO DO ESTADO DO PARÁ, inscrito no CNPJ/MF sob o nº 05.054.960/0001-58, estabelecido nesta Cidade à Rua João Diogo, 100, bairro Cidade Velha, CEP: 66015-165, doravante denominado **CONTRATANTE**, neste ato representado pelo Procurador-Geral de Justiça, Exmº. Sr. Dr., brasileiro,, residente e domiciliado em Belém e, de outro lado, a Empresa, portadora do CNPJ/MF nº., estabelecida à representada pelo(a) Sr(a).,, residente e domiciliado, doravante denominada **CONTRATADA**, têm por justo e contratado o que melhor se declara nas cláusulas e condições seguintes:

CLÁUSULA PRIMEIRA - DO FUNDAMENTO JURÍDICO

1.1. O presente Contrato decorre de licitação na modalidade **Pregão Eletrônico Nº 047/2020-MP/PA**, por execução indireta, empreitada por preço **global do lote/grupo**, no tipo menor preço, vinculada ao **PROCESSO Nº. 162/2019-SGJ-TA (PROTOCOLO Nº 45212/2019) e Ata de Registro de Preços XXX/2021-MP/PA**, e tem como fundamento as Leis Federais nº. 8.078/90 e 8.666/93 e na Lei Estadual nº 5.416/87, observadas as alterações e demais regras de direito público e privado aplicáveis a matéria que o subsidiarem.

1.2. Aos casos omissos serão aplicadas as normas referidas no subitem anterior.

CLÁUSULA SEGUNDA - DO OBJETO

2.1 O presente Contrato tem por objeto a **aquisição de**, solicitado no protocolo nº **xxxx/2021**, nas quantidades informadas na cláusula quarta

CLÁUSULA TERCEIRA - ESPECIFICAÇÃO DETALHADA DOS EQUIPAMENTOS E LICENÇAS

3.1. DESCRIÇÃO

3.1.1. Aquisição de solução de proteção de rede com características de Firewall Next Generation (NGFW) com SD-WAN integrada do tipo Appliance. A solução deve ser integralmente do mesmo fabricante, contemplando gerência centralizada, todos os softwares e suas licenças de uso, possibilitando atualização contínua. Deve incluir, além das funcionalidades citadas acima: Otimização de WAN, gerenciamento centralizada, zero-touch deployment, filtro de pacote, controle de aplicação, administração de largura de banda (QoS), VPN, IPSec e SSL, IPS, prevenção contra ameaças de vírus, spywares e malwares "Zero Day", Filtro de URL, bem como controle de transmissão de dados e acesso à internet compondo uma plataforma de segurança integrada e robusta. Na qual todos os links WANs e VPNs devem funcionar simultaneamente;

3.1.2. Por plataforma de segurança entende-se hardware e software integrados do tipo appliance com todas as licenças necessárias inclusas, o sistema operacional fornecido deve ser a versão mais nova disponível, devendo, entretanto, ser considerada estável pelo fabricante do equipamento;

3.1.3. A solução de NGFW deverá suportar mecanismos de redundância de dispositivos em modo ativo-passivo e ativo-ativo, em caso de falha de um dos equipamentos;

3.1.4. Deve possuir LEDs indicadores de status, atividade de rede, status dos links e alimentação;

3.1.5. O equipamento ofertado deve ser compatível com as seguintes funcionalidades:

3.1.5.1. Possibilitar a coleta de estatísticas de todo o tráfego que passar pelo firewall;

3.1.5.2. A solução deve apresentar informações de relatório de acordo com um intervalo de tempo definido pelo administrador;

3.1.5.3. A solução deve contemplar gerenciamento centralizado e integrado de todos os dispositivos da sede e filiais, que possibilite que as configurações, controle de acesso, regras e políticas

sejam executadas em um único ponto e replicadas para todos os dispositivos, grupos de dispositivos, usuários, grupos de usuários;

3.1.5.4. O equipamento deve permitir a gestão e monitoramento através da interface de gestão WEB no mesmo dispositivo de proteção da rede;

3.1.5.5. Permitir controle global e centralizado de políticas para todos os equipamentos que compõe a plataforma de segurança;

3.1.5.6. Exportar backup de configuração automaticamente via agendamento;

3.1.5.7. Os hardwares e softwares ofertados na composição deste item não devem estar listados como “end-of-sale”, “end-of-support” ou “end-of-life” por seus respectivos fabricantes na data da abertura das propostas. Não serão aceitos equipamentos que entrem em modo End of Support durante a vigência da garantia ou que entre em modo End of Life pelo período de 1 ano após a assinatura do contrato.

3.2. SD-WAN

3.2.1. Deve possuir capacidade para utilizar, pelo menos 3 (três) links de WAN, sendo no mínimo 2 (dois) links simultâneos.

3.2.2. Realizar balanceamento de tráfego de saída entre os links de Wan primários;

3.2.3. Permitir que a escolha do link WAN de saída seja influenciada por regras definidas pelo administrador de rede da CONTRATANTE e dinamicamente. As regras devem permitir ao menos um dos parâmetros a seguir ou combinação destes:

3.2.4. Endereço IP de origem e/ou destino;

3.2.5. Subredes de origem e/ou destino;

3.2.6. Métricas de Jitter, latência e perda de pacotes por aplicação;

3.2.7. Status da porta de WAN primários (UP ou DOWN);

3.2.8. Toda a comunicação Wan deve trafegar em um túnel VPN ponto-a-ponto estabelecido dinamicamente entre os PONTOS DE PRESENÇA da CONTRATANTE;

3.2.9. Suportar o protocolo de tunelamento GRE (General Routing Encapsulation - RFC 2784);

3.2.10. A solução deve ter um tempo máximo de failover e failback de 300 segundos;

3.2.11. A topologia da rede WAN deve ser dentre outras possíveis, a de malha completa (full mesh);

3.2.12. O estabelecimento do túnel VPN entre os PONTOS DE PRESENÇA pode inicialmente ser orientado pelo concentrador, mas o tráfego de dados após o estabelecimento do túnel deve ser realizado diretamente entre os integrantes do túnel, sem consumir throughput do concentrador;

3.2.13. A solução de SD-WAN deverá ser integrada no próprio appliance de NGFW, não sendo aceito quaisquer componentes adicionais com esta função.

CARACTERISTICAS GERAIS

3.3. Por cada equipamento que compõe a plataforma de segurança, entende-se o hardware e as licenças de softwares necessárias para o seu funcionamento;

3.4. Na data da proposta, nenhum dos modelos ofertados poderão estar listados como “end-of-sale”, “end-of-support” ou “end-of-life” por seus respectivos fabricantes. Não serão aceitos equipamentos que entrem em modo *End of Support* durante a vigência da garantia ou que entre em modo *End of Life* pelo período de 1 ano após a assinatura do contrato;

3.5. A solução deve consistir do *appliance* de proteção de rede com funcionalidades de Next Generation Firewall (NGFW) e SD-WAN, além de Solução de Gerência Centralizada com Sistema de Armazenamento de Log e Relatórios Centralizados;

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

3.7. As funcionalidades de proteção de rede (Firewall, IPS, Antivírus, Filtro Web, Controle de aplicações) que compõem a plataforma de segurança, devem funcionar localmente nos dispositivos NGFW;

3.8. A funcionalidade de *Sandbox* deve ser executada em nuvem pelo próprio fabricante, devendo o NGFW estar devidamente licenciado para possibilitar a execução desta função;

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

3.10. O hardware e software que executa as funcionalidades de proteção de rede firewall (NGFW) e SD-WAN deve ser do tipo *appliance*. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

- 3.11. Os *appliances* que executarão a função de NGFW deverão ter altura máxima de 1 (um) U de espaço em rack;
- 3.12. O software deverá ser fornecido em sua versão mais atualizada e estável;
- 3.13. Os equipamentos deverão ser fornecidos de acordo com as características técnicas mínimas presentes neste Termo de Referência;
- 3.14. A solução deverá ser capaz de fechar túneis VPN do tipo IPSec com equipamentos de terceiros (Palo Alto Networks, Cisco, Check Point, Juniper, Fortinet, SonicWall);
- 3.15. Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:
 - 3.15.1. Suporte a 4094 VLAN Tags 802.1q;
 - 3.15.2. Agregação de links 802.3ad e LACP;
 - 3.15.3. Policy based routing ou policy based forwarding;
 - 3.15.4. Roteamento multicast (PIM-SM e PIM-DM);
 - 3.15.5. DHCP Relay;
 - 3.15.6. DHCP Server;
 - 3.15.7. Jumbo Frames;
- 3.16. Os dispositivos de proteção de rede devem suportar *sFlow*;
- 3.17. Suportar sub-interfaces ethernet logicas.
- 3.18. Deve suportar os seguintes tipos de NAT:
 - 3.18.1. Nat dinâmico (Many-to-1);
 - 3.18.2. Nat dinâmico (Many-to-Many);
 - 3.18.3. Nat estático (1-to-1);
 - 3.18.4. NAT estático (Many-to-Many);
 - 3.18.5. Nat estático bidirecional 1-to-1;
 - 3.18.6. Tradução de porta (PAT);
 - 3.18.7. NAT de Origem;
 - 3.18.8. NAT de Destino;
 - 3.18.9. Suportar NAT de Origem e NAT de Destino simultaneamente.
 - 3.18.10. Deve implementar Network Prefix Translation (NPTv6), prevenindo problemas de roteamento assimétrico;
 - 3.18.11. Deve implementar o protocolo ECMP;
 - 3.18.12. Portas UDP, uma ou um range;
 - 3.18.13. Portas TCP, uma ou um range;
 - 3.18.14. Deve implementar balanceamento de link por hash do IP de origem;
 - 3.18.15. Deve implementar balanceamento de link por hash do IP de origem e destino;
 - 3.18.16. Deve implementar balanceamento de link através do método round-robin;
 - 3.18.17. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, três links;
 - 3.18.18. Deve implementar balanceamento de link através de políticas por usuário e grupos de usuários do LDAP/AD;
 - 3.18.19. Seleção do melhor caminho que o tráfego da sessão leva com base na qualidade do circuito baseado em Latência, Perda "Loss" e Jitter;
 - 3.18.20. A solução deve ser capaz de detectar perda, aumento de latência e jitter de um caminho, quando este começa a degradar a qualidade de uma aplicação. Deslocando o tráfego da aplicação para outro circuito de dado que esteja com melhor desempenho de forma transparente para os usuários, sem que seja percebido interrupção na continuidade do aplicativo ou dos pacotes perdidos;
 - 3.18.21. Deve implementar balanceamento de link através de políticas por aplicação, conforme regras de negócio;
 - 3.18.22. Deve implementar o protocolo Link Layer Discovery (LLDP), permitindo que o appliance e outros ativos da rede se comuniquem para identificação da topologia da rede em que estão conectados e a função dos mesmos facilitando o processo de troubleshooting. As informações aprendidas e armazenadas pelo appliance devem ser acessíveis via SNMP;
 - 3.18.23. Enviar log para sistemas de monitoração externos, simultaneamente;
 - 3.18.24. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;

3.18.25. Deve permitir configurar certificado caso necessário para autenticação no sistema de monitoração externo de logs;

3.18.26. Proteção contra anti-spoofing;

3.18.27. Deve permitir bloquear sessões TCP que usem variações do 3-way hand-shake, como 4 way e 5 way split hand-shake, prevenindo desta forma possíveis tráfegos maliciosos;

3.18.28. Deve exibir nos logs de tráfego o motivo para o término da sessão no firewall, incluindo sessões finalizadas onde houver de-criptografia de SSL e SSH;

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

3.18.30. Para IPv6, deve suportar roteamento estático e dinâmico (RIPv6, BGP4+, OSPFv3);

3.18.31. Suportar a OSPF graceful restart;

3.18.32. Suportar no mínimo as seguintes funcionalidades em IPv6: SLAAC (address auto configuration), NAT64, Identificação de usuários a partir do LDAP/AD, IPv6 over IPv4 IPsec, Regras de proteção contra DoS (Denial of Service), De-criptografia SSL e SSH, PBF (Policy Based Forwarding), QoS, DHCPv6 Relay, DHCPv6 Server, IPsec, Ativo/Ativo, Ativo/Passivo, SNMP, NTP, SYSLOG, DNS e controle de aplicação;

3.18.33. Dispositivos de proteção devem ter a capacidade de operar de forma simultânea em uma única instância de firewall, mediante o uso de suas interfaces físicas nos seguintes modos: Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);

3.18.34. Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;

3.18.35. Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;

3.18.36. Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;

3.18.37. Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;

3.18.38. Suporte à configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;

3.18.39. Em modo transparente;

3.18.40. Em Layer 3;

3.18.41. A configuração em alta disponibilidade deve sincronizar;

3.18.42. Sessões;

3.18.43. Configurações, incluindo, mas não limitado a políticas de Firewall, NAT, QOS e objetos de rede;

3.18.44. Certificados de-criptografados;

3.18.45. Associações de Segurança das VPNs;

3.18.46. Sincronizar tabelas FIB;

3.18.47. HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link;

O gerenciamento da solução deve suportar acesso via SSH e interface WEB (HTTPS), incluindo, mas não limitado à, exportar configuração dos sistemas virtuais (contextos) por ambas interfaces;

3.18.48. As funcionalidades de NGFW e SD-WAN, controle de aplicações, VPN IPsec e SSL, QOS, SSL e SSH Decryption e protocolos de roteamento dinâmico devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante.

3.19. CONTROLE POR POLÍTICA DE FIREWALL

3.19.1. Deverá suportar controles por zona de segurança;

3.19.2. O Firewall deverá possuir controles de segurança de camada L4 - L7;

3.19.3. A solução de firewall deve atuar na camada de aplicação possibilitando ao administrador criar regras e impedir a utilização de aplicações (*deep packet inspection*);

3.19.4. Controles de políticas por porta e protocolo;

3.19.5. Controle de políticas por aplicações grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;

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

3.19.7. Deve suportar a consulta a fontes externas de endereços IP, domínios e URLs podendo ser adicionados nas políticas de firewall para bloqueio ou permissão do tráfego;

3.19.8. Controle de políticas por código de País ou geolocalização (Por exemplo: BR, USA, UK, RUS);

3.19.9. Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (*Inbound*) e Saída (*Outbound*).

3.19.10. Deve suportar *offload* de certificado em inspeção de conexões SSL de entrada (*Inbound*);

3.19.11. Deve de-criptografar tráfego *Inbound* e *Outbound* em conexões negociadas com TLS 1.2;

3.19.12. Controle de inspeção e de-criptografia de SSH por política;

3.19.13. A de-criptografia de SSH deve possibilitar a identificação e bloqueio de tráfego caso o protocolo esteja sendo usado para tunelar aplicações como técnica evasiva para burlar os controles de segurança;

3.19.14. A plataforma de segurança deve implementar espelhamento de tráfego de-criptografado (SSL e TLS) para soluções externas de análise (Forense de rede, DLP, Análise de Ameaças, entre outras);

3.19.15. Bloqueios dos seguintes tipos de arquivos: bat, cab, dll, exe, pif e reg;

3.19.16. *Traffic shaping* QoS baseado em Políticas (Prioridade, Garantia e Máximo);

3.19.17. QoS baseado em políticas para marcação de pacotes (*diffserv marking*), inclusive por aplicações;

3.19.18. Suporte a objetos e regras IPV6;

3.19.19. Suporte a objetos e regras *multicast*;

3.19.20. Deve possibilitar a utilização de no mínimo 04 ações nas regras de controle como Permitir, Bloquear;

3.19.21. Deve suportar no mínimo os seguintes tipos de negação de tráfego nas políticas de firewall: *Drop* sem notificação do bloqueio ao usuário e TCP-Reset para o cliente;

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

3.19.23. O controle por políticas de firewall deverá ser integrado no próprio *appliance* de NGFW, não sendo aceito quaisquer componentes adicionais com esta função.

3.20. CONTROLE DE APLICAÇÕES

3.20.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;

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

3.20.3. Reconhecer pelo menos 2000 (duas mil) aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a *peer-to-peer*, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

3.20.4. Reconhecer pelo menos as seguintes aplicações: *bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, onedrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs, etc;*

3.20.5. Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações customizadas e não somente sobre aplicações conhecidas;

3.20.6. Deve inspecionar o *payload* de pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo. A checagem de assinaturas também deve determinar se uma aplicação está utilizando a porta default ou não, incluindo, mas não limitado a RDP na porta 80 ao invés de 389;

3.20.7. Deve aplicar heurística a fim de detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a *Encrypted Bittorrent* e aplicações VOIP que utilizam criptografia proprietária;

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

3.20.9. 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, incluindo, mas não limitado a Yahoo *Instant Messenger* usando HTTP. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação, incluindo, mas não limitado

a compartilhamento de arquivo dentro do Webex. Além de detectar arquivos e outros conteúdos que devem ser inspecionados de acordo as regras de segurança implementadas;

3.20.10. Deve permitir a utilização de aplicativos para um determinado grupo de usuário e bloquear para o restante, incluindo, mas não limitado a Skype. Deve permitir também a criação de políticas de exceção concedendo o acesso a aplicativos como Skype apenas para alguns usuários;

3.20.11. Identificar o uso de táticas evasivas via comunicações criptografadas;

3.20.12. Atualizar a base de assinaturas de aplicações automaticamente;

3.20.13. Reconhecer aplicações em IPv6;

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

3.20.15. 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 *Domain Controller*, nem nas estações dos usuários;

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

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

3.20.18. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão;

3.20.19. A criação de assinaturas personalizadas deve permitir o uso de expressões regulares, contexto (sessões ou transações), usando posição no *payload* dos pacotes TCP e UDP e usando decoders de pelo menos os seguintes protocolos: HTTP, FTP, SMTP, Telnet, SSH, MS-SQL, IMAP, MS-RPC e RTSP.

3.20.20. Deve alertar o usuário quando uma aplicação for bloqueada;

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

3.20.22. Deve possibilitar a diferenciação de tráfegos Peer2Peer (*Bittorrent*, *emule*, etc.) possuindo granularidade de controle/políticas para os mesmos;

3.20.23. Deve possibilitar a diferenciação de tráfegos para as seguintes aplicações e respectivas granularidades: Instagram (login, post, vídeo, upload de arquivo), YouTube (canais, streaming HD, pesquisa de vídeo, play vídeo), Facebook (upload e download de arquivos, login, chat, botão de like, chamadas VoIP, play vídeo, post, mensagem de voz), WhatsApp (transferência de arquivos, chamadas VoIP e whatsapp web);

3.20.24. Deve possibilitar a diferenciação de aplicações Proxies, possuindo granularidade de controle/políticas para os mesmos;

3.20.25. Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como: Tecnologia utilizada nas aplicações (Client-Server, Browser Based, Network Protocol, etc); Nível de risco da aplicação; Categoria de aplicações;

3.20.26. Deve ser possível configurar *Application Override* permitindo selecionar aplicações individualmente;

3.20.27. Aplicações que usem técnicas evasivas, utilizadas por *malwares*, como transferência de arquivos e/ou uso excessivo de banda, etc.

3.20.28. O controle de aplicações deverá ser integrado no próprio *appliance* de NGFW, não sendo aceito quaisquer componentes adicionais com esta função.

3.21. PREVENÇÃO DE AMEAÇAS

3.21.1. Para proteção do ambiente de redes contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio *appliance* de Firewall;

3.21.2. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);

3.21.3. As funcionalidades de IPS, Antivírus e *Anti-Spyware* devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;

- 3.21.4. Deve sincronizar as assinaturas de IPS, Antivírus, *Anti-Spyware* quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;
- 3.21.5. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS, *Anti-Spyware* e Antivírus: permitir, permitir e gerar log, bloquear, e enviar tcp-reset;
- 3.21.6. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;
- 3.21.7. Deve suportar granularidade nas políticas de IPS Antivírus e *Anti-Spyware*, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
- 3.21.8. Deve permitir o bloqueio de vulnerabilidades;
- 3.21.9. Deve permitir o bloqueio de *exploits* conhecidos;
- 3.21.10. Deve incluir proteção contra ataques de negação de serviços;
- 3.21.11. Fornecem proteção contra ataques de dia zero;
- 3.21.12. Deverá possuir os seguintes mecanismos de inspeção de IPS:
- 3.21.13. Análise de padrões de estado de conexões;
- 3.21.14. Análise de decodificação de protocolo;
- 3.21.15. Análise para detecção de anomalias de protocolo;
- 3.21.16. Análise heurística;
- 3.21.17. IP *Defragmentation*;
- 3.21.18. Remontagem de pacotes de TCP.
- 3.21.19. Bloqueio de pacotes malformados.
- 3.21.20. Ser imune e capaz de impedir ataques básicos como: Synflood, ICMPflood, UDPflood, etc;
- 3.21.21. Detectar e bloquear a origem de portscans;
- 3.21.22. Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;
- 3.21.23. Suportar os seguintes mecanismos de inspeção contra ameaças de rede: análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, análise heurística, IP *Defragmentation*, remontagem de pacotes de TCP e bloqueio de pacotes malformados;
- 3.21.24. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
- 3.21.25. Possuir assinaturas para bloqueio de ataques de *buffer overflow*;
- 3.21.26. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
- 3.21.27. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS e Anti-Spyware, permitindo a criação de exceções com granularidade nas configurações;
- 3.21.28. Permitir o bloqueio de vírus e *spywares* em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
- 3.21.29. Suportar bloqueio de arquivos por tipo;
- 3.21.30. Identificar e bloquear comunicação com *botnets*;
- 3.21.31. Deve suportar várias técnicas de prevenção, incluindo *Drop* e *tcp-rst* (Cliente, Servidor e ambos);
- 3.21.32. Deve suportar referência cruzada com CVE;
- 3.21.33. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:
- 3.21.33.1. O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 3.21.34. Deve suportar a captura de pacotes (PCAP) por assinatura de IPS;
- 3.21.35. Deve permitir que na captura de pacotes por assinaturas de IPS seja definido o número de pacotes a serem capturados. Esta captura deve permitir selecionar, no mínimo, 50 pacotes;
- 3.21.36. Deve possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos sejam resolvidas pelo Firewall com endereços (IPv4 e IPv6), previamente definidos;
- 3.21.37. Os eventos devem identificar o país de onde partiu a ameaça;
- 3.21.38. Deve incluir proteção contra vírus em conteúdo HTML e Java script, software espião (Spyware) e worms;

- 3.21.39. Proteção contra downloads involuntários usando HTTP de arquivos executáveis;
- 3.21.40. Rastreamento de vírus em pdf;
- 3.21.41. Deve permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, etc.);
- 3.21.42. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.
- 3.21.43. A prevenção de ameaças deverá ser integrada no próprio appliance de NGFW, não sendo aceito quaisquer componentes adicionais com esta função.

3.22. ANÁLISE DE MALWARE

- 3.22.1. Devido aos *Malwares* hoje em dia serem muito dinâmicos e um antivírus comum reativo não ser capaz de detectar os mesmos com a mesma velocidade que suas variações são criadas, a solução ofertada deve possuir funcionalidades para análise de Malwares não conhecidos incluídas na própria ferramenta ou entregue com composição com outro fabricante sem custo adicional;
- 3.22.2. O dispositivo de proteção deve ser capaz de enviar arquivos trafegados de forma automática para análise "*In Cloud*" ou local, onde o arquivo será executado e simulado em ambiente controlado;
- 3.22.3. Selecionar através de políticas granulares quais tipos de arquivos sofrerão esta análise incluindo, mas não limitado a: endereço IP de origem/destino, usuário/grupo do AD/LDAP, aplicação, porta, URL/categoria de URL de destino, tipo de arquivo e todas estas opções simultaneamente;
- 3.22.4. Deve possuir a capacidade de diferenciar arquivos analisados em pelo menos três categorias: malicioso, não malicioso e suspeito;
- 3.22.5. Suportar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Android, MacOS, Windows 8, Windows 7 (32 bits) e Windows 7 (64 bits), Windows 10 (32 bits) e Windows 10 (64 bits);
- 3.22.6. Deve suportar a monitoração de arquivos trafegados na internet (HTTPs, FTP, HTTP, SMTP) como também arquivos trafegados internamente entre servidores de arquivos usando SMB em todos os modos de implementação: *sniffer*, transparente e L3;
- 3.22.7. Para ameaças trafegadas em protocolo SMTP e POP3, a solução deve ter a capacidade de mostrar nos relatórios o remetente, destinatário e assunto dos e-mails permitindo identificação ágil do usuário vítima do ataque;
- 3.22.8. O sistema de análise "*In Cloud*" ou local deve gerar assinaturas de Antivírus e *Anti-Spyware* automaticamente, definir URLs não confiáveis utilizadas pelo novo Malware e prover informações sobre o usuário infectado (seu endereço ip e seu *login de rede*);
- 3.22.9. Caso a solução seja fornecida em *appliance* local, deve possuir, no mínimo, 28 ambientes controlados (*Sandbox*) independentes para execução simultânea de arquivos suspeitos;
- 3.22.10. Caso seja necessário, licenças de sistemas operacional e softwares para execução de arquivos no ambiente controlado (*Sandbox*), as mesmas devem ser fornecidas em sua totalidade, sem custos adicionais para a contratante;
- 3.22.11. Suportar a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado;
- 3.22.12. Deve atualizar a base com assinaturas para bloqueio dos malwares identificados em *Sandbox* com frequência;
- 3.22.13. A análise de Malware deverá ser integrada no próprio appliance de NGFW, não sendo aceito quaisquer componentes adicionais com esta função.

3.23. FILTRO URL

- 3.23.1. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
- 3.23.2. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, Ips, Redes e Zonas de segurança;
- 3.23.3. Incluir nativamente *Explicit Web Proxy* e *proxy Web* transparente;

3.23.4. Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via *ldap*, *Active Directory*, base de dados local, inclusive em modo de proxy transparente e explícito;

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

3.23.6. Suporta a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;

3.23.7. Deve bloquear o acesso a sites de busca (Google, Bing e Yahoo). O Firewall deve ter mecanismo que implemente a navegação com o uso o *Safe Search*, independente da intervenção do usuário.

3.23.8. Suporta base ou cache de URLs local no *appliance*, evitando *delay* de comunicação/validação das URLs;

3.23.9. Possui pelo menos 60 categorias de URLs;

3.23.10. A categorização de URL deve analisar toda a URL e não somente até o nível de diretório;

3.23.11. Suporta a criação categorias de URLs customizadas;

3.23.12. Suporta a criação de exceções nos bloqueios de filtro de URLs;

3.23.13. Permite a customização de página de bloqueio;

3.23.14. Permite o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão "Continuar" para permitir o usuário continuar acessando o site);

3.23.15. A funcionalidade de Filtro de URL, categorizada localmente, deve operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;

3.23.16. Suporta a inclusão nos logs do produto de informações das atividades dos usuários;

3.23.17. Deve possuir base ou cache de URLs local no *appliance* ou em nuvem do próprio fabricante, evitando *delay* de comunicação/validação das URLs;

3.23.18. Deve salvar nos logs as informações dos seguintes campos do cabeçalho HTTP nos acessos a URLs: UserAgent, Referer, e X-Forwarded For;

3.24. IDENTIFICAÇÃO DE USUÁRIOS

3.24.1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, *Active Directory*, e base de dados local;

3.24.2. Deve possuir integração com Microsoft *Active Directory* e LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

3.24.3. Deve possuir integração com *Radius* para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

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

3.24.5. Suporte a autenticação *Kerberos*;

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

3.24.7. Deve identificar usuários através de leitura do campo nos logs do firewall o endereço IP, bem como o usuário de rede responsável pelo acesso;

3.24.8. Deve permitir a criação de políticas de segurança baseadas em usuários de rede com reconhecimento dos mesmos através de leitura do campo de identificação do usuário;

3.24.9. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;

3.24.10. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em servidores acessados remotamente, mesmo que não sejam servidores Windows;

3.25. QOS

3.25.1. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, Ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de

máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming;

3.25.2. Suportar a criação de políticas de QoS e traffic-shaping por:

3.25.2.1. *Endereço de origem;*

3.25.2.2. *Endereço de destino;*

3.25.2.3. *Por usuário e grupo do LDAP/AD;*

3.25.2.4. *Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;*

3.25.2.5. *Por porta.*

3.25.3. QoS deve possibilitar a definição de classes por:

3.25.3.1. *Banda Garantida;*

3.25.3.2. *Banda Máxima;*

3.25.3.3. *Fila de Prioridade.*

3.25.4. Suportar priorização Real Time de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype;

3.25.5. Suportar marcação de pacotes *Diffserv*, inclusive por aplicação;

3.25.6. Deve implementar QoS (*traffic-shaping*), para pacotes marcados por outros ativos na rede (DSCP). A priorização e limitação do tráfego deve ser efetuada nos dois sentidos da conexão (*Inbound* e *Outbound*);

3.25.7. Disponibilizar estatísticas Real Time para classes de QoS;

3.25.8. Deve suportar QoS (*traffic-shaping*), em interface agregadas;

3.25.9. Deverá permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.

3.26. FILTRO DE DADOS

3.26.1. Permite a criação de filtros para arquivos e dados pré-definidos;

3.26.2. Os arquivos devem ser identificados por extensão, tipo e assinaturas (ou *fingerpint*);

3.26.3. Permite identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, SMTP, POP3, IMAP, MAPI, FTP e NNTP);

3.26.4. Suportar identificação de arquivos compactados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

3.26.5. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.

3.27. GEOLOCALIZAÇÃO

3.27.1. Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;

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

3.27.3. Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas.

3.28. VPN

3.28.1. Suportar VPN Site-to-Site e Cliente-To-Site;

3.28.2. Suportar IPSec VPN;

3.28.3. Suportar SSL VPN;

3.28.4. A VPN IPSec deve suportar:

3.28.5. *DES e 3DES;*

3.28.6. *Autenticação MD5 e SHA-1;*

3.28.7. *Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;*

3.28.8. *Algoritmo Internet Key Exchange (IKEv1 e v2);*

3.28.9. *AES 128, 192 e 256 (Advanced Encryption Standard);*

3.28.10. *Autenticação via certificado IKE PKI.*

3.28.11. Deve possuir interoperabilidade com os seguintes fabricantes: Palo Alto Networks, Cisco, Check Point, Juniper, Fortinet, SonicWall;

3.28.12. Deve permitir habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEc a partir da interface gráfica da solução, facilitando o processo de troubleshooting;

3.28.13. VPN SSL deve suportar:

3.28.13.1. Usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;

3.28.13.2. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente. Caso necessite de agente, deve estar licenciada para ou suportar sem o uso de licença, 50 (cinquenta) clientes de VPN SSL simultâneos;

3.28.13.3. Atribuição de endereço IP nos clientes remotos de VPN SSL;

3.28.13.4. Deve permitir a atribuição de IPs fixos nos usuários remotos de VPN SSL.

3.28.14. Deve permitir a criação de rotas de acesso e faixas de endereços IP atribuídas a clientes remotos de VPN de forma customizada por usuário AD/LDAP e grupo de usuário AD/LDAP;

3.28.15. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;

3.28.16. Atribuição de DNS nos clientes remotos de VPN;

3.28.17. Deve suportar autenticação de clientes VPN a partir de diferentes sistemas operacionais remotos (Android, IOS, Mac Windows e Chrome OS);

3.28.18. A solução de VPN deve verificar se o client que está conectando é o mesmo para o qual o certificado foi emitido inicialmente. O acesso deve ser bloqueado caso o dispositivo não seja o correto;

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

3.28.20. Suportar autenticação via AD/LDAP, OTP (One Time Password), certificado e base de usuários local;

3.28.21. Suporta leitura e verificação de CRL (certificate revocation list);

3.28.22. Permite a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;

3.28.23. Agente deverá comunicar-se com o portal para determinar as políticas de segurança do usuário;

3.28.24. Deve permitir que a conexão com a VPN SSL seja estabelecida das seguintes formas:

3.28.24.1. Antes do usuário autenticar na estação;

3.28.24.2. Após autenticação do usuário na estação;

3.28.24.3. Sob demanda do usuário.

3.28.25. Deverá manter uma conexão segura com o portal durante a sessão;

3.28.26. O agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows 7, Windows 8 e Mac Osx.

3.29. COMPATIBILIDADE

3.29.1. Todos os itens de hardware e software fornecidos pela PROPONENTE deverão ser da mesma marca e fabricante. A padronização da marca garante que os equipamentos adquiridos sejam 100% compatíveis entre si, permitindo a proteção de investimento a ser realizado por este órgão. Desta forma, faz-se necessária a aquisição de produtos de mesma marca e fabricante, com o fim de garantir a interoperabilidade e possibilidade de operar em Alta Disponibilidade entre si.

3.30. LICENCIAMENTO

3.30.1. Deve ser fornecido com a versão de software mais recente disponível para o equipamento;

3.30.2. Deve ser fornecido com todas as licenças de software necessárias para o funcionamento de todos os recursos descritos e exigidos neste termo para o prazo mínimo de 05 anos.

3.31. GARANTIA E SUPORTE

3.31.1. Durante o prazo de 05 anos, deve ser possível realizar a atualização de sistema operacional dos equipamentos, incluindo atualizações de novas assinaturas;

3.31.2. A garantia deve incluir envio de peças ou equipamentos de reposição nos locais especificados neste termo de referência, obedecendo a modalidade NBD (Next Business Day);

3.31.3. Os chamados poderão ser abertos diretamente com o fabricante ou autorizada pelo fabricante através de ligação telefônica 0800 no idioma Português, bem como via website e/ou e-mail durante a vigência da garantia (5 anos), sendo tais canais de comunicação informados pela CONTRATADA, por ocasião da assinatura da ARP/Contrato, indicando a empresa que prestará os serviços de garantia, com todas as informações necessárias (endereço completo, telefone, fax, e-mail e, se

houver, responsável técnico) através de declaração assinada pelo representante legal da mesma, específica para este pregão. A substituição da empresa indicada para a prestação da garantia on-site somente poderá ser feita mediante comunicação e autorização prévia do Ministério Público do Estado do Pará.

3.31.4. O suporte deverá ser na modalidade de 24x7 (24 horas por dia, 7 dias por semana), com atendimento através de ligação telefônica para atendimentos emergenciais.

3.32. DOS ITENS DO LOTE 01

3.32.1. Item 01 - NGFW de pequeno porte com SD-WAN integrada, garantia, suporte e todas as licenças necessárias: 134 (cento e trinta e quatro) unidades.

3.32.1.1. CAPACIDADE E QUANTIDADE

3.32.1.1.1. Throughput de, no mínimo, 02 (dois) Gbps com a funcionalidade de firewall habilitada;

3.32.1.1.2. Throughput de no mínimo 450 (quatrocentos e cinquenta) Mbps com a funcionalidade de controle de aplicação e logs habilitada;

3.32.1.1.3. Throughput de no mínimo 160 (cento e sessenta) Mbps com as seguintes funcionalidades habilitadas: controle de aplicação, IPS, Antivírus e Anti-Spyware e log. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, todas deverão ter valor superior ao throughput requerido;

3.32.1.1.4. Capacidades (throughput) comprovadas por documento de domínio público disponibilizado pelo fabricante, não sendo admitida a comprovação de Throughput para funcionalidades de camada 7 (Controle de Aplicação e IPS, por exemplo), com tráfego UDP e/ou RFCs baseadas neste protocolo;

3.32.1.1.5. Efetividade de Segurança mínima de 80%, classificados como recomendado em Security Value Map (SVM) Comparative Report para Next Generation Firewall (NGFW) da NSS Labs ou certificação ICASA Labs para o ano de 2018 ou posterior, seja para o modelo apresentado ou para equipamento da mesma linha que possua mesmo sistema operacional e engine de anti-vírus, comprovada por documento de domínio público;

3.32.1.1.6. Suporte a, no mínimo, 192 (Cento e noventa e dois) mil conexões simultâneas;

3.32.1.1.7. Suporte a, no mínimo, 13 (treze) mil novas conexões por segundo;

3.32.1.1.8. Fonte de alimentação automática 100-240V AC;

3.32.1.1.9. Possuir espaço em disco SSD interno com no mínimo 32 (trinta e dois) GB;

3.32.1.1.10. No mínimo 7 (sete) interfaces de rede gigabit Ethernet RJ45, devendo ser possível configurar ao menos 02 (duas) destas interfaces como WAN;

3.32.1.1.11. 01 (uma) interface do tipo console ou similar;

3.32.1.1.12. Suporte a, no mínimo, 20 (vinte) zonas de segurança;

3.32.1.1.13. Estar licenciada para suportar sem o uso de licença, 200 (duzentos) clientes de VPN SSL simultâneos;

3.32.1.1.14. Estar licenciada para suportar sem o uso de licença, 200 (duzentos) túneis de VPN IPSEC simultâneos.

3.32.2. Item 02 - NGFW de médio porte com SD-WAN integrada, garantia, suporte e todas as licenças necessárias: 20 (vinte) unidades

3.32.2.1. CAPACIDADE E QUANTIDADE

3.32.2.1.1. Throughput de, no mínimo, 10 (dez) Gbps com a funcionalidade de firewall habilitada;

3.32.2.1.2. Throughput de no mínimo 02 (dois) Gbps com a funcionalidade de controle de aplicação e logs habilitada;

3.32.2.1.3. Throughput de no mínimo 700 (setecentos) Mbps com as seguintes funcionalidades habilitadas simultaneamente: controle de aplicação IPS, Antivírus e Anti-Spyware e logs. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, todas deverão ter valor superior ao throughput requerido;

3.32.2.1.4. Capacidades (throughput) comprovadas por documento de domínio público disponibilizado pelo fabricante, não sendo admitida a comprovação de Throughput para funcionalidades de camada 7 (Controle de Aplicação e IPS, por exemplo), com tráfego UDP e/ou RFCs baseadas neste protocolo;

3.32.2.1.5. Efetividade de Segurança mínima de 80%, classificados como recomendado em Security Value Map (SVM) Comparative Report para Next Generation Firewall (NGFW) da NSSLabs ou certificação ICSA Labs para o ano de 2018 ou posterior, seja para o modelo apresentado ou para equipamento da mesma linha que possua mesmo sistema operacional e engine de anti-vírus, comprovada por documento de domínio público; Suporte a, no mínimo, 1,5 (um vírgula cinco) milhão de conexões simultâneas;

3.32.2.1.6. Suporte a, no mínimo, 50 (cinquenta) mil novas conexões por segundo;

3.32.2.1.7. Fonte de alimentação automática 100-240V AC;

3.32.2.1.8. Possuir espaço em disco SSD interno com no mínimo 240 (duzentos e quarenta)

GB;

3.32.2.1.9. No mínimo 10 (dez) interfaces de rede gigabit Ethernet RJ45, devendo ser possível configurar ao menos 02 (duas) destas interfaces como WAN;

3.32.2.1.10. No mínimo 08 (oito) slots SFP;

3.32.2.1.11. No mínimo 02 (dois) slots SFP+;

3.32.2.1.12. 01 (uma) interface do tipo console ou similar;

3.32.2.1.13. Fonte de alimentação automática 100-240V AC;

3.32.2.1.14. Suporte a, no mínimo, 06 (seis) sistemas virtuais lógicos (Contextos) no firewall físico. Os contextos virtuais devem suportar as funcionalidades nativas do gateway de proteção incluindo: Firewall, IPS, Antivírus, Anti-Spyware, Filtro de URL, Filtro de Dados, VPN, Controle de Aplicações, QoS, NAT e Identificação de usuários;

3.32.2.1.15. Suporte a, no mínimo, 50 (cinquenta) zonas de segurança;

3.32.2.1.16. Estar licenciada para ou suportar sem o uso de licença, 400 (quatrocentos) clientes de VPN SSL simultâneos;

3.32.2.1.17. Estar licenciada para ou suportar sem o uso de licença, 02 (dois) mil túneis de VPN IPSEC simultâneos.

3.32.3. Item 03 - NGFW concentrador de VPN com SD-WAN integrada, garantia, suporte e todas as licenças necessárias: 02 (duas) unidades em HA (Alta Disponibilidade)

3.32.3.1. CAPACIDADE E QUANTIDADE

3.32.3.1.1. Throughput de, no mínimo, 36 (trinta e seis) Gbps com a funcionalidade de firewall habilitada;

3.32.3.1.2. Throughput de no mínimo 15 (quinze) Gbps com a funcionalidade de controle de aplicação habilitada;

3.32.3.1.3. Throughput de no mínimo 07 (sete) Gbps com as seguintes funcionalidades habilitadas simultaneamente: controle de aplicação IPS, Antivírus e Anti-Spyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, todas deverão ter valor superior ao throughput requerido;

3.32.3.1.4. Capacidades (throughput) comprovadas por documento de domínio público disponibilizado pelo fabricante, não sendo admitida a comprovação de Throughput para funcionalidades de camada 7 (Controle de Aplicação e IPS, por exemplo), com tráfego UDP e/ou RFCs baseadas neste protocolo;

3.32.3.1.5. Efetividade de Segurança mínima de 80%, classificados como recomendado em Security Value Map (SVM) Comparative Report para Next Generation Firewall (NGFW) da NSSLabs ou certificação ICSA Labs para o ano de 2018 ou posterior, seja para o modelo apresentado ou para equipamento da mesma linha que possua mesmo sistema operacional e engine de anti-vírus, comprovada por documento de domínio público;

3.32.3.1.6. Suporte a, no mínimo, 7,5 (sete vírgula cinco) milhões de conexões simultâneas;

3.32.3.1.7. Suporte a, no mínimo, 280 (duzentos e oitenta) mil novas conexões por segundo;

3.32.3.1.8. Fontes de alimentação automáticas 100-240V AC, redundante;

3.32.3.1.9. Possuir espaço em disco SSD interno com no mínimo 240 (duzentos e quarenta)

GB;

3.32.3.1.10. No mínimo 08 (oito) interfaces de rede gigabit Ethernet RJ45, devendo ser possível configurar ao menos 02 (duas) destas interfaces como WAN;

3.32.3.1.11. No mínimo 06 (seis) slots SFP;

3.32.3.1.12. No mínimo 02 (dois) slots SFP+;

3.32.3.1.13. 01 (uma) interface do tipo console ou similar;

3.32.3.1.14. Suporte a, no mínimo, 06 (seis) sistemas virtuais lógicos (Contextos) no firewall físico. Os contextos virtuais devem suportar as funcionalidades nativas do gateway de proteção incluindo: Firewall, IPS, Antivírus, Anti-Spyware, Filtro de URL, Filtro de Dados, VPN, Controle de Aplicações, QoS, NAT e Identificação de usuários;

3.32.3.1.15. Suporte a, no mínimo, 100 (cem) zonas de segurança;

3.32.3.1.16. Estar licenciada para suportar sem o uso de licença, 09 (nove) mil clientes de VPN SSL simultâneos;

3.32.3.1.17. Estar licenciada para suportar sem o uso de licença, 02 (dois) mil túneis de VPN IPSEC simultâneos.

3.32.4. Item 04 - SISTEMA DE GERÊNCIA CENTRALIZADA

3.32.4.1. Deve prover gestão centralizada dos dispositivos denominados PONTOS DE PRESENÇA, e ser necessariamente do mesmo fabricante do NGFW;

3.32.4.2. Por console de gerência, entende-se as licenças de software necessárias para esta funcionalidade;

3.32.4.3. Deve estar licenciado e suportar a gestão de, no mínimo, 160 (cento e sessenta) dispositivos denominados PONTOS DE PRESENÇA;

3.32.4.4. Deve ser do tipo Appliance Físico, Appliance Virtual ou solução de software baseada em máquina virtual (VM). Caso seja baseada em Máquina Virtual (VM), a PROPONENTE deverá indicar em sua proposta qual a necessidade de hardware a ser disponibilizada pelo CONTRATANTE para a respectiva instalação;

3.32.4.5. Caso seja em VM, deve ser compatível com VMware ESX(i);

3.32.4.6. Possuir ao menos 4 (quatro) interfaces de rede VNIC;

3.32.4.7. Deve estar licenciado para suporta ao menos 5GB Log/dia + 1TB (Cinco Gigabyte de Log por dia e 01 Terabyte);

3.32.4.8. Deve suportar operação em alta disponibilidade (há) sincronizando as mudanças na base de dados entre as estações de gerência;

3.32.4.9. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;

3.32.4.10. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;

3.32.4.11. Permitir acesso concorrente de administradores;

3.32.4.12. Possuir interface baseada em linha de comando para administração da solução de gerência;

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

3.32.4.14. Bloqueio de alterações, no caso de acesso simultâneo de dois ou mais administradores;

3.32.4.15. Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;

3.32.4.16. Gerar alertas automáticos via Email;

3.32.4.17. Gerar alertas automáticos via SNMP;

3.32.4.18. Deve suportar backup/restore de todas as configurações da solução de gerência, permitindo ao administrador agendar backups da configuração em um determinado dia e hora;

3.32.4.19. Deve ser permitido ao administrador transferir os backups para um servidor FTP;

3.32.4.20. As alterações realizadas em um servidor de gerência deverão ser automaticamente replicadas para o servidor redundante;

3.32.4.21. Deve ser permitido aos administradores se autenticarem nos servidores de gerência através de contas de usuários LOCAIS;

3.32.4.22. Deve ser permitido aos administradores se autenticarem nos servidores de gerência através de usuários de base externa LDAP;

3.32.4.23. Deve ser permitido aos administradores se autenticarem nos servidores de gerência através de base externa RADIUS;

3.32.4.24. Deve ser permitido aos administradores se autenticarem nos servidores de gerência através de Certificado Digital X.509 (PKI);

3.32.4.25. Deve suportar sincronização do relógio interno via protocolo NTP;

- 3.32.4.26. Deve registrar as ações efetuadas por quaisquer usuários;
- 3.32.4.27. Devem ser fornecidos manuais de instalação, configuração e operação de toda a solução, na língua portuguesa ou inglesa, com apresentação de boa qualidade;
- 3.32.4.28. Suportar SNMP versão 2 e versão 3 nos equipamentos de gerência;
- 3.32.4.29. Deve permitir virtualizar a solução de gerência, de forma que cada administrador possa gerenciar, visualizar e editar apenas os dispositivos autorizados e cadastrados no seu ambiente virtualizado;
- 3.32.4.30. A solução de gerência deve permitir criar administradores que tenham acesso à todas as instâncias de virtualização;
- 3.32.4.31. Deve suportar XML API;
- 3.32.4.32. O gerenciamento deve possibilitar a criação e administração de políticas de firewall e controle de aplicação;
- 3.32.4.33. O gerenciamento deve possibilitar a criação e administração de políticas de IPS, Antivírus e Anti-Spyware;
- 3.32.4.34. O gerenciamento deve possibilitar a criação e administração de políticas de Filtro de URL;
- 3.32.4.35. Permitir localizar quais regras um objeto está sendo utilizado;
- 3.32.4.36. Deve atribuir sequencialmente um número a cada regra de firewall;
- 3.32.4.37. Deve atribuir sequencialmente um número a cada regra de DOS;
- 3.32.4.38. Permitir criação de regras que fiquem ativas em horário definido;
- 3.32.4.39. Permitir backup das configurações e rollback de configuração para a última configuração salva;
- 3.32.4.40. Deve possuir mecanismo de Validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);
- 3.32.4.41. Deve possibilitar a visualização e comparação de configurações atuais, configuração anterior e configurações antigas;
- 3.32.4.42. Deve permitir que todos os firewalls sejam controlados de forma centralizada utilizando apenas um servidor de gerência;
- 3.32.4.43. O servidor de gerência deve ser hospedado em um equipamento independente, não exercendo funções de firewall;
- 3.32.4.44. A solução deve incluir uma ferramenta para gerenciar centralmente as licenças de todos os appliances controlados pela estação de gerenciamento, permitindo ao administrador atualizar licenças nos appliances através dessa ferramenta;
- 3.32.4.45. A solução deve possibilitar a distribuição e instalação remota, de maneira centralizada, de novas versões de software dos appliances;
- 3.32.4.46. Deve ser capaz de gerar relatórios ou exibir comparativos entre duas sessões diferentes, resumindo todas as alterações efetuadas;
- 3.32.4.47. Permitir visualizar, a partir da estação de gerência centralizada, informações detalhadas dos dispositivos gerenciados, tais como hostname, serial, IP de gerência, licenças, horário do sistema e firmware;
- 3.32.4.48. Permitir criar os objetos que serão utilizados nas políticas de forma centralizada.

3.32.5. Item 05 - Serviço de Instalação/Configuração

- 3.32.5.1. Os equipamentos concentradores e o Sistema de Gerência Centralizada devem ser instalados no prédio sede do Ministério Público do Pará - MPPA (Rua João Diogo, nº 100 – Cidade Velha - 66.015.165 Belém/PA). Além dos equipamentos e sistema citados acima, este item contempla a instalação de um NGFW em cada uma das unidades relacionadas no Anexo II Localidades;
- 3.32.5.2. Reunião inicial: deverá ser realizada uma reunião inicial entre o gestor do contrato e a PROPONENTE, cuja pauta observará, pelo menos:
 - 3.32.5.2.1. Assinatura da Carta de Confidencialidade;
 - 3.32.5.2.2. Esclarecimentos relativos a questões operacionais e de gerenciamento do contrato;
 - 3.32.5.2.3. Estrutura organizacional da CONTRATANTE;
 - 3.32.5.2.4. Infraestrutura de TI da CONTRATANTE;
- 3.32.5.3. A CONTRATADA deverá prestar serviços de instalação e configuração, que compreendem, entre outros, os seguintes procedimentos:

3.32.5.3.1. Análise da topologia e arquitetura da rede, considerando os roteadores, servidores de aplicação e firewall já existentes e instalados;

3.32.5.3.2. Análise do acesso Internet, sites remotos, serviços de rede oferecidos aos funcionários e aos usuários externos;

3.32.5.3.3. Regras de Firewall existentes e aplicáveis solução ofertada dada a colocação desta na Rede deste parquet;

3.32.5.3.4. Análise do posicionamento de qualquer outro equipamento ou sistema relevante na segurança de qualquer perímetro protegido pela solução;

3.32.5.3.5. Apresentação do plano de implantação com o descritivo de todos os serviços a serem executados e topologia física e lógica a ser implementada;

3.32.5.3.6. Configuração do sistema de Firewall, SD-WAN, VPN, IPS, Filtro URL, Antivírus e Anti-Malware de acordo com as exigências levantadas com as devidas atualizações necessárias;

3.32.5.3.7. Instalação de Sistema de Gerência Centralizada em Appliance Físico, Appliance Virtual ou solução baseada em VM (máquina virtual), de acordo com a oferta da CONTRATADA. O mesmo será considerado entregue, quando for instalado e configurado na sede do MPPA, com todas as atualizações, configurações e licenças. Deverão ser adicionados a este todos os pontos de presença do Anexo I e Concentradores, cujos deverão estar sendo monitorados e gerenciados por este Sistema de Gerência Centralizada;

3.32.5.4. Deve haver geração de relatório e entrega da documentação da instalação com as configurações efetuadas e as decisões tomadas, diagramas e topologias em formato legível e tecnicamente fundamentado;

3.32.5.5. O recebimento definitivo consiste no aceite dos produtos e/ou serviços além do atendimento aos termos e condições do Edital, Contrato e seus anexos, inclusive a proposta comercial da PROPONENTE.

3.32.5.6. O aceite poderá ser parcial, ou seja, se acordo com a entrega de cada item adquirido.

3.32.6. Item 06 - Treinamento “Hands On” sobre Solução de Firewall/SD-WAN

3.32.6.1. A CONTRATADA deverá ministrar treinamento do tipo “Hands On” sobre a solução de Firewall/SD-WAN adquirida, incluindo instalação, configuração básica e avançada, troubleshoot, monitoramento e gerenciamento;

3.32.6.2. A carga horária mínima será de 20 horas divididas em expedientes de 4h/dia, das 8h às 12h;

3.32.6.3. O treinamento será ministrado para um total de seis (6) participantes do quadro de pessoal do Ministério Público definidos pela CONTRATANTE;

3.32.6.4. O repasse deverá ter caráter prático e se baseará no sistema Firewall/SD-WAN efetivamente instalado na CONTRATANTE;

3.32.6.5. O treinamento deve ser do tipo presencial e a sua realização será na cidade de Belém (Pará) nas dependências do Ministério Público. A CONTRATANTE irá ceder uma sala, um projetor e computadores, com acesso à internet, para sua realização. É de responsabilidade da CONTRATADA designar um profissional certificado pelo Fabricante, fornecer todo material audiovisual, didático e, caso necessário, outros equipamentos eletrônicos para a realização dos treinamentos, além de impressos. Todos os demais custos, ônus, obrigações e encargos para o treinamento devem ser arcados pela CONTRATADA.

CLÁUSULA QUARTA - DO PREÇO, DA QUANTIDADE E DOS RECURSOS FINANCEIROS

4.1. O valor global do presente contrato é de R\$ (.....), conforme o disposto na proposta da Contratada, datada de .../.../2021, pela execução do objeto, nas especificações, quantidade e preços unitários abaixo:

- Inserir planilha com as descrição, quantidade e preços unitários.

Parágrafo Único – No valor estabelecido nesta cláusula estão incluídos todos os tributos, contribuições fiscais e parafiscais previstos na legislação em vigor incidentes, direta ou indiretamente e despesas de quaisquer natureza decorrentes da execução do presente contrato.

4.2. Para atender às despesas do presente Contrato, o Ministério Público, valer-se-á de recursos orçamentários na função programática:

Classificação: 12101.03.122.1494.8760 – Governança e Gestão

Elemento: 4490-52 – Equipamentos e Material Permanente

Fonte: 0301 – Recursos Ordinários

Elemento: 3390-40 – Serviços da Tecnologia da Informação e Comunicação

Fonte: 0101 – Recursos Ordinários

CLÁUSULA QUINTA - DAS CONDIÇÕES DE PAGAMENTO

5.1. O pagamento será efetuado pelo Departamento Financeiro do Ministério Público no prazo máximo de **30 (trinta) dias** corridos, no Banco: xxxxxx, Agência nº xxxxx, Conta Corrente nº xxxx, salvo atraso na liberação de recursos pela Secretaria Executiva de Planejamento, Orçamento e Finanças - SEPOF, após o recebimento definitivo **da solução e dos serviços licitados**, mediante a apresentação **das Notas Fiscais devidamente atestadas** pelo FISCAL, o qual observará as especificações exigidas.

5.1.1. O pagamento dos fornecedores de bens e prestadores de serviços dos órgãos da Administração Direta e Indireta do Estado do Pará será efetuado mediante crédito em conta corrente aberta no Banco do Estado do Pará S/A – BANPARÁ, conforme Decreto Estadual nº 877, de 31/03/2008.

5.1.2. Caso o prestador não possua conta no banco BANPARÁ, será cobrada pelo banco taxa referente ao DOC/TED, sendo o valor desta taxa automaticamente descontado no valor depositado para pagamento da prestação do serviço.

5.1.3. Pagamentos através de código de barra só poderão ser realizados caso a empresa possua convênio com o Banco do Estado do Pará (BANPARÁ), uma vez que todos os pagamentos são realizados através do SIAFEM (Sistema Integrado de Administração Financeira de Estados e Municípios).

5.2. O atesto da nota fiscal será efetuado no prazo máximo de 05 (cinco) dias úteis contados do recebimento definitivo do material pelo responsável pela Fiscalização no local anteriormente mencionado;

5.3. A nota fiscal que contiver erro será devolvida à contratada para retificação e reapresentação, iniciando a contagem dos prazos fixados para o ATESTO a partir do recebimento da Nota Fiscal corrigida.

5.4. A CONTRATADA deverá encaminhar, junto com a nota fiscal, os seguintes documentos:

5.4.1. Certidão conjunta negativa de débitos relativos aos tributos federais e a dívida ativa da União;

5.4.2. Certidão negativa de débitos relativos às Contribuições Previdenciárias;

5.4.3. Certificado de regularidade do FGTS – CRF;

5.4.4. Certidão negativa de débitos inadimplidos perante a Justiça do Trabalho;

5.4.5. Certidão negativa de débitos com Fazenda Estadual;

5.4.6. Certidão negativa de débitos com a Fazenda Municipal;

5.5. Ocorrendo erro no documento da cobrança, este será devolvido e o pagamento será susgado para que a CONTRATADA tome medidas necessárias, passando o prazo para o pagamento a ser contado a partir da data da reapresentação do mesmo.

5.6. Não efetuado o pagamento pelo CONTRATANTE no prazo estabelecido na sub-cláusula 5.1, e desde que não haja culpa da CONTRATADA, os valores correspondentes à fatura serão atualizados financeiramente com base no critério abaixo especificado, em observância ao art. 40, XIV, “c” da Lei 8.666/93 e suas alterações.

$EM = I \times N \times VP$

Onde:

EM=Encargos Monetários

N=Número de dias entre a data prevista para o pagamento e do efetivo pagamento

VP=Valor da parcela a ser paga

I=Índice de atualização financeira = 0,0001644, assim apurado:

$I = \frac{(TX/100)}{365}$ $I = \frac{(6/100)}{365}$ $I = 0,0001644$

TX=Percentual da taxa anual=6%

CLÁUSULA SEXTA – DOS ACRÉSCIMOS E SUPRESSÕES E DEMAIS ALTERAÇÕES

6.1. Nos itens a partir de 04 unidades, a contratada fica obrigada a aceitar, nas mesmas condições contratuais, os acréscimos e supressões até 25% (vinte e cinco por cento) do valor inicial atualizado do contrato, referentes à alteração quantitativa do item, nos termos do art. 65, § 1º, da Lei nº. 8.666/93, salvo a exceção prevista no § 2º do referido artigo

6.2. Este instrumento poderá ainda ser alterado, exceto no objeto, nos termos do art. 65 da Lei 8.666/93 e com as devidas justificativas, nos seguintes casos:

I - Unilateralmente pela Administração:

- a) quando houver modificação do projeto ou das especificações, para melhor adequação técnica aos seus objetivos;
- b) quando necessária a modificação do valor contratual em decorrência de acréscimo ou diminuição quantitativa de seu objeto, nos limites permitidos por esta Lei;

II - Por acordo das partes:

- a) quando conveniente a substituição da garantia de execução;
- b) quando necessária a modificação do regime de execução da obra ou serviço, bem como do modo de fornecimento, em face de verificação técnica da inaplicabilidade dos termos contratuais originários;
- c) quando necessária a modificação da forma de pagamento, por imposição de circunstâncias supervenientes, mantido o valor inicial atualizado, vedada a antecipação do pagamento, com relação ao cronograma financeiro fixado, sem a correspondente contraprestação de fornecimento de bens ou execução de obra ou serviço;
- d) para restabelecer a relação que as partes pactuaram inicialmente entre os encargos do contratado e a retribuição da administração para a justa remuneração da obra, serviço ou fornecimento, objetivando a manutenção do equilíbrio econômico-financeiro inicial do contrato, na hipótese de sobrevirem fatos imprevisíveis, ou previsíveis porém de consequências incalculáveis, retardadores ou impeditivos da execução do ajustado, ou, ainda, em caso de força maior, caso fortuito ou fato do príncipe, configurando álea econômica extraordinária e extracontratual.

CLÁUSULA SÉTIMA – DO REAJUSTE

7.1. O valor proposto e contratado poderá ser reajustado, em consonância com as disposições desta Cláusula.

7.1.1. Caso assim queira, a contratada deverá requerer o reajustamento do preço, mediante protocolo no Ministério Público do Estado do Pará, até a data em que se completar cada período de 12 (doze) meses de vigência do contrato, sob pena de preclusão quanto ao período correspondente.

7.1.2. A data-base para o cálculo do reajuste é a data da apresentação da proposta.

7.1.3. Para o cálculo do reajuste, deverá ser adotado o IGP-DI (da Fundação Getúlio Vargas), em sua variação para o período de 12 (doze) meses, a contar da data-base referida no item 7.1.2.

7.1.4. O valor reajustado será concedido somente a partir da data de cada prorrogação, ainda que posterior à anualidade da proposta, e observados os itens anteriores.

7.2. Se a contratada requerer o reajustamento do preço em conformidade com o item 7.1.1, mas o valor reajustado ainda não puder ser concedido na data da prorrogação contratual, por indisponibilidade do índice para a variação referida no item 7.1.3, constará do termo aditivo de prorrogação a ressalva do direito da contratada ao reajuste do preço, que ocorrerá efetivamente mediante termo específico e quando houver aquela disponibilidade, com retroatividade à data de cada prorrogação.

7.3. Não serão admitidos requerimentos de reajustes para períodos preclusos

CLÁUSULA OITAVA - DOS PRAZOS E CONDIÇÕES DE ENTREGA, RECEBIMENTO E GARANTIA

8.1. CONTRATADA se compromete a efetuar a entrega dos produtos solicitados no prazo não superior a 60 (sessenta) dias corridos, a contar do início da vigência do contrato.

8.2. A entrega dos produtos será no Edifício Sede do Ministério Público, sito na Rua João Diogo, n. 100 – 2º andar, Cidade Velha, Belém, Pará, no horário das 08h00min às 14h00min, de segunda a

sexta-feira, exceto nos feriados e dias facultativos, correndo por conta da contratada todas as despesas de embalagem, seguros, transporte, tributos, encargos trabalhistas e previdenciários, decorrentes do serviço e equipamentos necessários para o seu funcionamento, devendo a entrega ser agendada, com até 48h de antecedência, pelos telefones (91) 4006-3480/3481;

8.3. O CONTRATADO terá prazo de 06 (seis) dias úteis a contar da comunicação para retirar a Nota de Empenho de Despesas ou instrumento equivalente.

8.4. Os equipamentos deverão ser novos (de primeiro uso), e deverão ser entregues devidamente protegidos e adequadamente embalados contra danos de transporte manuseio e acompanhados das notas fiscais de remessa;

8.5. Caso se veja impossibilitada de cumprir com o prazo estipulado no item 4.1, a Contratada deverá, por escrito e com antecedência mínima de 10 (dez) dias corridos antes de expirado o prazo, solicitar prorrogação do prazo e apresentar justificativas;

8.6. O pedido de prorrogação, com indicação do novo prazo, quando for o caso, deverá ser encaminhado à fiscalização da Contratante, que poderá, de modo justificado, acolher ou não o pedido;

8.7. Vencidos os prazos de entrega ou de prorrogação e não cumprida a obrigação de entrega, a Contratante oficiará a Contratada acerca do transcurso da data limite, passando o inadimplemento, a partir daí, a ser considerado como recusa do cumprimento da obrigação pactuada e, por conseguinte, sujeitando a empresa às penalidades prevista na lei;

8.8. O recebimento do objeto pela FISCALIZAÇÃO ou COMISSÃO DE RECEBIMENTO (nas compras acima de R\$ 80.000,00) se dará em duas etapas:

a) Em caráter provisório, imediatamente após a entrega dos equipamentos (item 1 a 3) e serviços (itens 4 a 6), representada pela conferência da quantidade e da qualidade do material entregue (está em sentido da aparência da embalagem) e conformidade com o modelo indicado na proposta comercial, com a entrega do sistema e verificação da conformidade com as informações prestadas na proposta comercial, o funcionamento básico dos equipamentos instalados e a conclusão da carga-horária do treinamento;

b) Definitivamente, em até 10 (dez) dias úteis a contar do recebimento provisório, mediante análise individual, que comprove sua conformidade com os padrões estabelecidos no presente Edital;

c) Os objetos serão recebidos e conferidos pela Fiscalização/Comissão de Recebimento designada por esta Instituição.

8.9. O objeto somente será considerado entregue quando emitido o Termo de Recebimento Definitivo dos Bens pela Contratante;

8.10. Se, após o recebimento provisório, constatar-se que os equipamentos foram entregues em desacordo com o solicitado, fora da especificação ou incompletos, após a notificação à Contratada, será suspenso o pagamento até que sanada a situação, independente de aplicação de sanções cabíveis;

8.11. O recebimento do material não exclui a responsabilidade administrativa, civil e penal da empresa por problemas causados durante o uso dos itens adquiridos nem exclui a responsabilidade da CONTRATADA pelo perfeito desempenho do objeto fornecido, cabendo-lhe sanar quaisquer irregularidades detectadas quando de sua utilização;

8.12. A Contratada e/ou detentora da ata deve promover, às suas expensas, a substituição total ou parcial do objeto que apresentar qualquer irregularidade;

8.13. Em caso de qualquer inconformidade, a Contratada terá prazo máximo de 30 (trinta) dias corridos após notificação emitida pela Contratante para sanar quaisquer pendências encontradas, sob pena de aplicação das sanções cabíveis;

8.14. Na hipótese de ser verificada a impropriedade do material no ato da entrega, o mesmo será imediatamente rejeitado, no todo ou em parte, a critério da FISCALIZAÇÃO responsável pelo recebimento, sendo o fornecedor notificado a proceder à substituição no prazo máximo de 30 (trinta) dias corridos, contados da ciência da rejeição, sendo-lhe, ainda, concedidos 05 (cinco) dias úteis para retirada do material ou parte do que foi rejeitado;

8.15. Os profissionais responsáveis pela implantação da solução e treinamento devem ser certificados pelo fabricante da solução;

8.16. A Contratada deverá promover, às suas expensas, a substituição total ou parcial do objeto que apresentar qualquer irregularidade.

8.17. O prazo de garantia será de, no mínimo, 60 (SESSENTA) meses, contados a partir da data do aceite definitivo. A garantia será prestada on-site na sede do MP/PA.

8.18. Os serviços de garantia e suporte técnicos deverão ser prestados aos equipamentos existentes nas dependências do Departamento de Informática – Edifício Sede do MP/PA, 2º Andar, Rua João Diogo, 100, Cidade Velha, Belém, Pará, CEP 66.015.165, assegurando-se, sem ônus para o CONTRATANTE, a cobertura para defeitos de fabricação, pelo período mínimo de 60 (Sessenta) meses, englobando equipamentos, peças e serviços, contados da data em que ocorrer o recebimento definitivo dos bens;

8.19. Durante a vigência dos serviços, chamados técnicos, sem limite de quantidade, poderão ser abertos, no horário de 00:00 às 23:59 horas, de segunda-feira a domingo, via discagem direta gratuita (linha 0800), ou via sistema próprio, em sítio na Internet, caracterizando a abertura do chamado;

8.20. O suporte técnico, deverão ser mantidas pelo prazo definido nas especificações de cada item;

8.21. Os serviços de Suporte e Garantia do equipamento devem ser em regime de 5x8xNBD, modalidade Next Business Day (próximo dia útil comercial), durante o período mínimo de 60 (sessenta) meses para toda a solução, contados da data em que ocorrer recebimento definitivo dos bens;

8.22. O uso da modalidade remota não afeta de forma alguma a contagem dos prazos estipulados;

8.23. O problema dos equipamentos defeituosos, caso comprovado, deverá ser sanado dentro dos tempos estipulados. Quando não for possível solucionar o problema no prazo estipulado, caso autorizado após avaliação por representante do Departamento de Informática, deverá ser fornecido outro equipamento de igual configuração ou superior, até resolução definitiva do problema;

8.24. A CONTRATADA, no momento da assinatura do Contrato, deverá fornecer número de telefone e/ou endereço de site na internet da central de atendimento para abertura de chamados;

8.25. Os chamados deverão ser resolvidos em até 3 (três) dias úteis, contados do primeiro dia útil seguinte à abertura do mesmo. Findo o prazo de 3 (três) dias úteis, sem a resolução do problema, deverá a CONTRATADA disponibilizar em até 24 horas equipamento de especificação igual ou superior para operação temporária como substituição do equipamento em conserto, o qual deverá ser avaliada e autorizado por representante do Departamento de Informática, não ultrapassando o prazo máximo de 30 (trinta) dias para a solução definitiva do problema;

8.26. O serviço de garantia será prestado com vistas a manter os equipamentos fornecidos em perfeitas condições de uso, sem qualquer ônus adicional para o Ministério Público do Estado do Pará. Nesse sentido, a garantia deve englobar:

a) A remoção dos vícios apresentados pelos equipamentos, materiais, drivers e outros componentes que sejam disponibilizados pelo fabricante dos equipamentos;

b) Solução de problemas e esclarecimento de dúvidas de configuração e de utilização dos equipamentos;

8.27. Os serviços deverão ocorrer de acordo com instruções a serem dadas pelo Departamento de Informática ou por servidor designado para esse fim. A realização dos serviços previstos, a serem efetuados nas dependências do Ministério Público do Estado do Pará, por funcionário da CONTRATADA, deverá ser acompanhada por profissional designado pelo Departamento de Informática do Ministério Público do Estado do Pará;

8.28. As atividades de prestação de serviços de garantia aos equipamentos deverão ocorrer em dias úteis, no período de 8 (oito) às 14 (quatorze) horas;

8.29. Durante todo o período da prestação de serviços de suporte técnico, a CONTRATADA deverá fornecer ao Contratante um usuário e senha para acesso ao sítio do Fabricante na Internet, onde deverá ser possível acompanhar o licenciamento instalado e, em área própria para o modelo ofertado, recursos para consulta e download de:

8.29.1. Softwares, drivers e firmwares (atualizações e/ou versões completas);

8.29.2. Manuais de usuário e dos equipamentos;

8.29.3. Banco de solução para suporte ao software e hardware instalados de fábrica.

8.30. A CONTRATADA deverá manter controle dos chamados abertos, registrando durante toda a vigência contratual ao menos as seguintes informações: número do chamado, número de série do equipamento, data de abertura do chamado, responsável pela abertura do chamado no MPPA, descrição do chamado, local da prestação dos serviços, peças substituídas, data de fechamento do chamado e responsável pela aprovação do fechamento do chamado no MPPA;

8.31. A CONTRATADA deverá indicar, quando da assinatura do contrato, a empresa que prestará os serviços de garantia, com todas as informações necessárias (endereço completo, telefone, fax, e-mail e,

se houver, responsável técnico) através de declaração assinada pelo representante legal da mesma, específica para este pregão. A substituição da empresa indicada para a prestação da garantia on-site somente poderá ser feita mediante comunicação e autorização prévia do Ministério Público do Estado do Pará;

8.32. Durante o período da prestação de serviços de garantia e suporte técnico, devem ser disponibilizados e instalados, sem ônus à Contratante, todas as atualizações de software e firmware para os equipamentos, quando for necessário;

8.33. Todos os equipamentos deverão ser previamente registrados pelo fornecedor junto ao fabricante, em nome da Contratante, caso seja uma exigência para fins de garantia;

8.34. Substituir qualquer equipamento durante o prazo de suporte se, em um período de 6 (seis) meses, ocorrer mais de 3 (três) chamados referentes ao mesmo problema (desde que a causa-raiz do mesmo tenha sido atribuída ao equipamento), ou mais de 5 (cinco) chamados referentes a problemas distintos (desde que a causa-raiz dos mesmos tenha sido atribuída ao equipamento);

8.35. A CONTRATADA deve fornecer opção de abertura de ocorrências através de sistema via WEB e através de telefone. O sistema via web, deve ser protegido por senha, permitir a abertura de ocorrências, geração automática do número da ocorrência e o envio automático de correio eletrônico (e-mails) para o pessoal envolvido. Os atendimentos referentes à instalação, análise de performance e ajuste de configurações serão realizados mediante agendamento prévio entre o pessoal técnico responsável da CONTRATANTE e da CONTRATADA. Ao término de cada atendimento a CONTRATADA deve gerar relatório descrevendo as atividades realizadas e o tempo gasto para tal, este relatório deve ser aprovado pela CONTRATADA.

8.36. Quando da assinatura do contrato, comprovar **através de documentação do fabricante** que os equipamentos especificados para os itens 01 a 03 são novos e de primeiro uso, e que não estarão fora da linha de produção nos próximos **120 (cento e vinte) dias** após a entrega dos mesmos;

8.37. Caso os produtos entregues não sejam de fabricação nacional, deverá ser apresentada original ou cópia autenticada da Declaração de Importação, emitida pela Receita Federal;

8.38. Relativamente, ao disposto nesta cláusula, aplicam-se também, subsidiariamente, no que couber, as disposições da Lei nº 8.078 de 11/09/90 – Código de Defesa do Consumidor;

8.39. Entrega dos Serviços de Instalação/Configuração:

8.39.1. O serviço de Instalação/Configuração deve ser executado no máximo após 30 dias da entrega dos equipamentos;

8.39.2. O Serviço de Instalação/Configuração será dado como entregue com o atendimento de todos os itens e subitens descritos no tópico 3.32.5. “Item 05 - Serviço de Instalação/Configuração”;

8.39.3. Entrega do plano de implantação atualizado, aprovado pela equipe técnica do MPPA com o descritivo de todos os serviços que foram executados, contendo topologia física, lógica e endereçamento implementado;

8.39.4. Instalação física e configuração de todos os equipamentos adquiridos no local determinado pela equipe de TI no anexo II, conforme plano de implantação com todas as atualizações e configurações do sistema de Firewall, SD-WAN, VPN, IPS, Filtro URL, Antivírus e Anti-Malware de acordo com os requisitos levantados;

8.39.5. A migração de todas as regras de Firewall, VPN, IPS, Filtro URL, Antivírus e Anti-Malware do dispositivo antigo para o novo firewall;

8.39.6. Entrega do relatório de instalação e configuração, contendo toda documentação das instalações e configurações efetuadas, as decisões tomadas, diagramas e topologias em formato legível e tecnicamente fundamentado;

8.39.7. Aceite do **item** Instalação/Configuração pelo fiscal ou suplente do contrato.

8.40. Entrega do Serviço Treinamento:

8.40.1. A entrega do serviço deve atender todos os itens descritos no tópico 3.32.6. Item 06 - Treinamento “Hands On” sobre Solução de Firewall/SD-WAN;

8.40.2. O serviço denominado Treinamento deve ser iniciado no primeiro dia útil após a conclusão do serviço de Instalação/Configuração e finalizado no prazo máximo de 15 dias corridos a contar da conclusão da instalação/configuração dos equipamentos;

8.40.3. O treinamento deve ser ministrado em língua portuguesa e deve ser realizado com material didático em PDF, elaborado pelo fabricante ou CONTRATADA;

8.40.4. A parte prática deve ser executada, nas dependências do Ministério Público, que fornecerá, à equipe própria de trabalho, computadores e acesso à internet para desenvolvimento das atividades em ambiente de teste virtual ou on-line disponibilizado pelo fabricante ou pela contratada por este homologado;

8.40.5. A CONTRATADA deve informar com antecedência mínima de 05 dias úteis, requisitos específicos para realização do treinamento, tais como: acesso a domínios, protocolos, portas, serviços, ips, dentre outros;

8.40.6. O treinamento deverá ser do tipo “*hands on training*”, com foco prático na implantação, configuração básica e avançada, troubleshoot, monitoramento e gerência da solução de Firewall/SD-WAN fornecida pela CONTRATADA, e também baseado no caso concreto das necessidades deste Parquet;

8.40.7. O certificado deve conter a carga horária do curso (20 horas) e ser entregue pela CONTRATADA até 05 dias após a conclusão do curso;

8.40.8. Ocasão em que será feita a conferência, pelo Departamento de Informática, da quantidade de horas ministradas e verificação da conformidade dos itens exigidos neste instrumento;

8.40.9. O não cumprimento dos prazos acima, sujeitará a CONTRATADA em mora, cujo atraso computar-se-á desde o primeiro dia do vencimento do prazo;

8.40.10. O serviço de Treinamento “Hands On” será considerado entregue após a conclusão de 20 horas aulas e entrega do certificado;

8.40.11. Na hipótese de ser verificada a impropriedade do treinamento ministrado, o mesmo será rejeitado, no todo ou em parte, a critério da FISCALIZAÇÃO responsável pelo seu recebimento, sendo o fornecedor obrigado a refazer o treinamento no prazo máximo de 15 (quinze) dias úteis após a verificação sem qualquer ônus para a Administração, independentemente da aplicação das penalidades cabíveis;

CLÁUSULA NONA – DA VIGÊNCIA DO CONTRATO

9.1. Este O presente Instrumento terá vigência de **05 (cinco) meses**, contados da data da publicação deste instrumento no Diário Oficial do Estado do Pará, **não podendo ser prorrogado**, salvo se ocorrer qualquer um dos motivos do art. 57 §1º, da lei 8.666/93, que implique a prorrogação dos prazos de execução e, conseqüentemente, exija a prorrogação da vigência do contrato, observado o caput do mesmo dispositivo legal.

CLÁUSULA DÉCIMA - DOS DIREITOS E DAS OBRIGAÇÕES DO CONTRATANTE

- 10.1. Sem que a isto limite seus direitos, terá o Ministério Público as seguintes garantias:
- 10.1.1. Receber o objeto de acordo com o que consta neste instrumento;
 - 10.1.2. Devolver o objeto em desacordo com as especificações exigidas.
- 10.2. Sem que a isto limite sua responsabilidade, será o Órgão responsável pelos seguintes itens:
- 10.2.1. Cumprir e fazer cumprir o disposto nas condições deste instrumento;
 - 10.2.2. Cumprir todos os compromissos financeiros assumidos com a CONTRATADA no prazo estipulado;
 - 10.2.3. Proporcionar todas as facilidades, inclusive esclarecimentos atinentes ao objeto, para que a empresa possa cumprir as obrigações dentro das normas e condições da aquisição;
 - 10.2.4. Indicar servidor com competência necessária para proceder o recebimento dos objetos e atestar as Notas Fiscais após a verificação das especificações, qualidade, quantidade e preços pactuados;
 - 10.2.5. Promover, através de seu representante, o acompanhamento e a fiscalização do objeto contratado, sob os aspectos quantitativos e qualitativos, prazos de vigência e entregas, anotando em registro próprio as falhas detectadas e comunicando ao Órgão por escrito as advertências e as ocorrências de quaisquer fatos que, a seu critério, exijam medidas corretivas por parte desta;
 - 10.2.6. Emitir nota de empenho a crédito do fornecedor no valor correspondente à quantidade solicitada;
 - 10.2.7. Acompanhar e fiscalizar a perfeita execução do CONTRATO;
 - 10.2.8. Efetuar o pagamento à CONTRATADA referente à quantia efetivamente entregue e após o cumprimento das formalidades legais, no prazo máximo de 30 (trinta) dias corridos contados do atesto da respectiva nota fiscal do material entregue.

CLÁUSULA DÉCIMA PRIMEIRA - DOS DIREITOS E DAS OBRIGAÇÕES DA CONTRATADA

11.1. Sem que a isto limite suas garantias, a CONTRATADA terá os seguintes direitos:

11.1.1. Receber informações e esclarecimentos necessários ao cumprimento das condições estabelecidas;

11.1.2. Receber o Atesto do recebimento do objeto contratado após verificação das especificações;

11.1.3. Receber formalmente a notificação de ocorrência de irregularidades que a fiscalização identificar na execução do objeto, até para que possa a empresa proceder correções;

11.1.4. Receber o pagamento nas condições estabelecidas neste instrumento.

11.2. Sem que a isto limite sua responsabilidade, será a CONTRATADA responsável pelos seguintes itens:

11.2.1. Cumprir fielmente as obrigações assumidas, conforme as especificações, zelando pela fiel execução, utilizando-se de todos os recursos materiais e humanos necessários;

11.2.2. Fornecer o objeto em estrita conformidade com as especificações e condições exigidas, bem como naquelas resultantes de sua proposta, devendo já estar inclusos nos valores propostos todos os custos, impostos, taxas e demais encargos pertinentes à formação do preço;

11.2.3. Entregar os equipamentos e manuais e os prospectos em português no prazo, local e horário previstos no Contrato, observando rigorosamente as exigências estabelecidas nas especificações e na proposta de preços apresentada pela empresa;

11.2.4. Durante o recebimento, substituir o equipamento não aceito pela Contratante em prazo não superior a 30 (trinta) dias corridos, contados da ciência da rejeição;

11.2.5. Responsabilizar-se pelo ônus de retirada e devolução dos equipamentos para realização de serviços de suporte técnico fora das dependências da Contratante;

11.2.6. A CONTRATADA é obrigada a reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, o objeto desta contratação em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou de materiais empregados;

11.2.7. Arcar com todas as despesas, diretas ou indiretas, decorrentes do cumprimento das obrigações assumidas, responsabilizando-se pelos danos causados diretamente à administração ou a terceiros, decorrentes de sua culpa ou dolo, por ocasião da entrega dos objetos no local indicado, incluindo os possíveis danos causados por transportadoras, sem qualquer ônus ao contratante.

11.2.8. Ser responsável pelos encargos trabalhistas, previdenciários, fiscais e comerciais resultantes da execução; a inadimplência da CONTRATADA, com referência aos encargos estabelecidos neste item não transfere a responsabilidade por seu pagamento à Administração do Ministério Público, nem poderá onerar o objeto desta contratação, razão pela qual a CONTRATADA renuncia expressamente a qualquer vínculo de solidariedade, ativa ou passiva, com o Ministério Público;

11.2.9. Quando da assinatura do contrato, comprovar através de documentação do fabricante que os equipamentos especificados para os itens 01 a 03 são novos e de primeiro uso, e que não estarão fora da linha de produção nos próximos 120 (cento e vinte) dias após a entrega dos mesmos;

11.2.10. Caso os produtos entregues não sejam de fabricação nacional, deverá ser apresentada original ou cópia autenticada da Declaração de Importação, emitida pela Receita Federal;

11.2.11. Prestar todos os esclarecimentos que forem solicitados pelo Ministério Público, durante o prazo de fornecimento, credenciando, junto ao Órgão, um representante para prestar os devidos esclarecimentos e atender as reclamações que porventura surgirem durante a execução;

11.2.12. Manter durante todo o prazo de vigência da relação obrigacional com a Contratante a regularidade com o fisco, com o sistema de seguridade social, com a legislação trabalhista, normas e padrões de proteção ao meio ambiente e cumprimento dos direitos da mulher, inclusive os que protegem a maternidade, sob pena da rescisão contratual, sem direito a indenização conforme preceitua o art. 28, §4º da Constituição do Estado do Pará, assim como todas as leis e posturas federais, estaduais e municipais, vigentes, sendo a única responsável por prejuízos decorrentes de infrações a que houver dado causa.

11.2.13. Quando, por problemas, técnicos os prazos pactuados não puderem ser cumpridos, a CONTRATADA deverá comunicar por escrito ao Órgão até 02 (dois) dias úteis anteriores ao término do prazo, ao qual caberá aceitar ou rejeitar as justificativas;

11.2.14. Manter, durante toda a execução, todas as condições de habilitação e qualificação exigidas no Pregão que sejam compatíveis com as obrigações a serem assumidas:

- 11.2.14.1. Regularidade Fiscal com a Fazenda Nacional, o Sistema de Seguridade Social e o Fundo de Garantia do Tempo de Serviço – FGTS;
- 11.2.14.2. Regularidade Fiscal perante as Fazendas Estaduais e Municipais da sede da licitante;
- 11.2.14.3. Regularidade Trabalhista;
- 11.2.14.4. Cumprimento do disposto no art. 7º, XXXIII, da Constituição Federal/88 (trabalho de menores de idade, observada a Lei nº 9.854/1999);
- 11.2.15. Informar o Órgão de qualquer alteração necessária à consolidação dos ajustes decorrentes da execução do objeto, tais como: mudança de endereço, razão social, telefone, fax, dissolução da sociedade, falência e outros;
- 11.2.16. Assumir inteira responsabilidade técnica e administrativa do objeto ADJUDICADO, não podendo, sob qualquer hipótese, transferir a outras empresas a responsabilidade por problemas de funcionamento;
- 11.2.17. Respeitar e obedecer às normas fixadas pela Administração da CONTRATANTE;
- 11.2.18. O inadimplemento das obrigações da CONTRATADA, com referência aos encargos trabalhistas, previdenciários, fiscais e comerciais, resultantes da execução, não transfere à Administração da CONTRATANTE a responsabilidade por seu pagamento, nem pode onerar o objeto deste Termo;
- 11.2.19. Não transferir a outrem, no todo ou em parte, o objeto do presente, sem prévia e expressa anuência do Ministério Público;
- 11.2.20. A CONTRATADA é obrigada a reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou de materiais empregados.
- 11.2.21. Responder por acidentes de que possam ser vítimas seus profissionais e, ainda, por eventuais danos causados no local entrega do objeto, aos servidores da CONTRATANTE, bem como a terceiros, quando praticados, por dolo, negligência, imperícia ou imprudência, diretamente por seus empregados na execução do ajuste, arcando, após regular processo administrativo, com a restauração, substituição ou indenização, conforme o caso, devendo os funcionários da empresa contratada apresentarem documentos (RG e CPF) para que seja providenciada a autorização de acesso aos locais indicados na nota de empenho;
- 11.2.22. Comunicar imediatamente à Administração, bem como ao responsável pela fiscalização, qualquer anormalidade verificada, inclusive de ordem funcional, para que sejam adotadas as providências de regularização necessárias, em qualquer tempo até o final da garantia;
- 11.2.23. Quando da prestação do eventual serviço de garantia ao equipamento:
- 11.2.23.1. Fazer-se representar, no local da prestação do eventual serviço de Garantia, por preposto aceito pela Administração com a atribuição de coordenar e fiscalizar a execução dos serviços e o cumprimento das normas disciplinares, de segurança e legislação pertinentes;
- 11.2.23.2. Atender prontamente às chamadas e às determinações do representante da Administração da CONTRATANTE com vistas a corrigir defeitos observados nos equipamentos entregues dentro do prazo de garantia;
- 11.2.23.3. Utilizar pessoal técnico qualificado, devidamente identificado com crachás contendo nome, foto e cargo/função desempenhada nas dependências da CONTRATANTE;
- 11.2.23.4. Comprovar, quando solicitado, a qualificação técnica dos funcionários que irão atender o MPPA;
- 11.2.23.5. Assumir a responsabilidade por todas as providências e obrigações estabelecidas na legislação específica de acidentes do trabalho, quando, em ocorrência da espécie, forem vítimas os seus empregados no desempenho dos serviços de Assistência Técnica ou em conexão com eles, ainda que acontecido nas dependências da CONTRATANTE;
- 11.2.24. Assumir todos os encargos sobre demanda trabalhista, previdenciários, obrigações sociais previstas na legislação social e trabalhista em vigor, cível ou penal, relacionado ao eventual serviço de Garantia, originariamente ou vinculados por prevenção, conexão ou contingência, além de assumir a responsabilidade pelos encargos fiscais e comerciais;
- 11.2.25. São de responsabilidade da CONTRATADA todas e quaisquer despesas decorrentes de sua atividade;
- 11.2.26. Observar a Resolução nº 172/2017-CNMP que altera o artigo 3º, caput, da Resolução CNMP nº 37/2009 e VEDA ao Ministério Público a contratação das pessoas jurídicas que tenham em seu quadro societário cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade até o terceiro grau, inclusive, dos membros ocupantes de cargos de direção ou no exercício de funções administrativas,

assim como de servidores ocupantes de cargos de direção, chefia e assessoramento vinculados direta ou indiretamente às unidades situadas na linha hierárquica da área encarregada da licitação;

11.2.26.1. A vedação do item 11.2.27 não se aplica às hipóteses nas quais a contratação seja realizada por ramo do Ministério Público diverso daquele ao qual pertence o membro ou servidor gerador da incompatibilidade.

11.2.26.2. A vedação do item 11.2.27 se estende às contratações cujo procedimento licitatório tenha sido deflagrado quando os membros e servidores geradores de incompatibilidade estavam no exercício dos respectivos cargos e funções, assim como às licitações iniciadas até 6 (seis) meses após a desincompatibilização.

11.2.26.3. A contratação de empresa pertencente a parente de membro ou servidor não abrangido pelas hipóteses expressas de nepotismo poderá ser vedada pelo órgão do Ministério Público competente, quando, no caso concreto, identificar risco potencial de contaminação do processo licitatório.

11.2.27. Aceitar o fato de que as informações obtidas em decorrência da execução do presente Termo deverão ser mantidas em sigilo, não podendo qualquer participante divulgá-las fora do âmbito deste instrumento, exceto se previamente acordado por escrito, ou prevista a sua divulgação.

11.2.28. Observar a VEDAÇÃO de contratação de Empresa que tenha entre seus empregados colocados à disposição do Ministério Público para o exercício de funções de chefia, pessoas que incidam na vedação dos arts. 1º e 2º da **Resolução nº 177/2017-CNMP**:

11.2.28.1. Pessoa que tenha sido condenada em decisão com trânsito em julgado ou proferida por órgão jurisdicional colegiado, nos seguintes casos:

I – atos de improbidade administrativa;

II – crimes:

a) contra a administração pública;

b) contra a incolumidade pública;

c) contra a fé pública;

d) contra o patrimônio;

e) de abuso de autoridade, nos casos em que houver condenação à perda do cargo ou à inabilitação para o exercício de função pública;

f) de tráfico de entorpecentes e drogas afins, racismo, tortura, terrorismo e hediondos;

g) contra a vida e a dignidade sexual;

h) praticados por organização ou associação criminosa;

i) de redução de pessoa à condição análoga à de escravo;

j) eleitorais, para os quais a lei comine pena privativa de liberdade;

k) de lavagem ou ocultação de bens, direitos e valores.

11.2.28.2. Aqueles que tenham:

I – praticado atos causadores da perda do cargo ou emprego público, reconhecidos por decisão transitada em julgado ou proferida por órgão judicial colegiado;

II – sido excluídos do exercício da profissão, por decisão definitiva sancionatória judicial ou administrativa do órgão profissional competente, salvo se o ato houver sido anulado ou suspenso pelo Poder Judiciário;

III – tido suas contas relativas ao exercício de cargos ou funções públicas rejeitadas por irregularidade insanável que configure ato doloso de improbidade administrativa, por decisão irreversível do órgão competente, salvo se esta houver sido suspensa ou anulada pelo Poder Judiciário, devendo tal condição constar expressamente dos editais de licitação.

CLÁUSULA DÉCIMA SEGUNDA –DA GARANTIA DE EXECUÇÃO DO CONTRATO (somente para contratos a partir de R\$100.000,00)

12.1. A **CONTRATADA** deverá prestar a garantia de execução do contrato, **no valor de R\$......, equivalente a 5% do contrato**, nos moldes do art. 56 da Lei nº 8.666, de 1993, com validade durante a execução do contrato e 90 (noventa) dias após término da vigência contratual, devendo ser renovada a cada prorrogação, observados ainda os seguintes requisitos:

12.1.1. A contratada deverá apresentar, no prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, a critério do órgão contratante, contado da assinatura do contrato, comprovante de

prestação de garantia, podendo optar por caução em dinheiro ou títulos da dívida pública, seguro-garantia ou fiança bancária;

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

- i. Prejuízos advindos do não cumprimento do objeto do contrato;
- ii. Prejuízos diretos causados à Administração decorrentes de culpa ou dolo durante a execução do contrato;
- iii. Multas moratórias e punitivas aplicadas pela Administração à contratada; e
- iv. Obrigações trabalhistas e previdenciárias de qualquer natureza, não adimplidas pela contratada, quando couber.

12.1.3. A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados no subitem 12.1.2 acima, observada a legislação que rege a matéria;

12.1.4. A garantia em dinheiro deverá ser efetuada no **Banco do Estado do Pará** em conta específica com correção monetária, em favor do contratante;

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

12.1.6. O atraso superior a 15 (quinze) dias autoriza a Administração a promover a rescisão do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõem os incisos I e II do art. 78 da Lei nº 8.666, de 1993;

12.1.7. O garantidor não é parte para figurar em processo administrativo instaurado pelo contratante com o objetivo de apurar prejuízos e/ou aplicar sanções à contratada;

12.1.8. A garantia será considerada extinta:

- i. Com a devolução da apólice, carta-fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração da Administração, mediante termo circunstanciado, de que a contratada cumpriu todas as cláusulas do contrato; e
- ii. Com o término da vigência do contrato, observado o prazo previsto no subitem 12.1 acima, que poderá, independentemente da sua natureza, ser estendido em caso de ocorrência de sinistro.

12.1.9. O contratante executará a garantia na forma prevista na legislação que rege a matéria;

12.2. O Contratante fica autorizado a utilizar a garantia para corrigir as imperfeições na execução do Objeto deste contrato ou reparar danos decorrentes da ação ou omissão do Contratado ou de preposto seu ou, ainda, para satisfazer qualquer obrigação resultante ou decorrente de suas ações ou omissões.

12.3. O Contratado se obriga a repor, no prazo de 48 (quarenta e oito) horas, o valor da garantia que vier a ser utilizado pelo Contratante.

12.4. Em caso de acréscimo ao valor contratual, por meio de termo aditivo, o Contratado fica obrigado a prestar garantia adicional de 5% sobre o valor acrescido;

12.4.1. A garantia prestada será retida definitivamente, integralmente ou pelo saldo que apresentar, no caso de rescisão por culpa do Contratado, sem prejuízo das penalidades cabíveis.

12.4.2. A garantia será restituída, automaticamente ou por solicitação, somente após integral cumprimento de todas as obrigações contratuais, inclusive recolhimento de multas e satisfação de prejuízos causados ao Contratante.

12.4.3. Em se tratando de modalidade fiança bancária, deverá constar do instrumento a expressa renúncia pelo fiador dos benefícios previstos nos arts. 827 e 835 do Código Civil.

CLÁUSULA DÉCIMA TERCEIRA – DAS PENALIDADES

13.1. Pela inexecução total ou parcial do contrato a Administração poderá, garantida a prévia defesa, aplicar ao contratado as sanções previstas nos art. 86 e 87 da lei 8.666/93, conforme segue:

13.2. ADVERTÊNCIA

13.2.1. Advertência, no caso de descumprimento de Cláusula Contratual que não interfira na execução dos serviços ou na sua conclusão e não traga sérios prejuízos econômicos e funcionais a este Órgão;

13.3. MULTA

13.3.1. De 0,25% ao dia, até o limite máximo de 5%, sobre o valor total **do item solicitado**, nos casos de atraso injustificado nos prazos de **retirada/aceite da nota de empenho**.

13.3.1.1. Após o 20º dia de atraso dos prazos previstos, sem justificativa aceita pela Administração, o objeto será considerado como inexecutado.

13.3.2. De 0,25% ao dia, até o limite máximo de 5%, sobre o valor total **da respectiva nota de empenho**, nos casos de atraso injustificado nos prazos **entrega do objeto; substituição do objeto**.

13.3.2.1. Após o 20º dia de atraso dos prazos previstos, sem justificativa aceita pela Administração, o objeto será considerado como inexecutado.

13.3.3. De 10%, sobre o valor total **do item solicitado**, nos casos de:

I. Recusa injustificada em retirar/aceitar a **nota de empenho**, se configurar inexecução total;

13.3.4. De 10%, sobre o valor total **da respectiva nota de empenho**, nos casos de:

I. Recusa injustificada em **entregar/executar o objeto**, se configurar inexecução total;

II. Recusa injustificada em substituir o objeto recusado ou com vícios, se configurar inexecução total;

III. Outras hipóteses de inexecução total do objeto.

13.3.5. De 10%, sobre o valor total **da respectiva nota de empenho**, nos casos de:

I. Recusa injustificada em retirar/aceitar a nota de empenho, se configurar inexecução parcial;

II. Entregar/executar parcial o objeto;

III. Recusa injustificada em substituir o objeto recusado ou com vícios, se configurar inexecução parcial;

IV. Outras hipóteses de inexecução parcial do objeto.

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

13.3.7. De 5% sobre o valor total **da respectiva nota de empenho** nos casos de irregularidade no cumprimento do objeto ou na prestação da garantia do produto do objeto contratado, não referidas nos itens anteriores

13.3.8. As multas são autônomas e a aplicação de uma não exclui a outra;

13.3.9. Havendo garantia à execução apresentada pela empresa, o valor da multa será descontado da mesma. Não havendo garantia ou caso o valor da multa seja superior à referida, a multa ou a diferença será cobrada administrativamente pela Contratante, podendo ser descontado dos créditos devidos, ou ainda judicialmente.

13.4. SUSPENSÃO

13.4.1. Nos casos de inexecução total ou parcial ou irregularidade não justificada e/ou não aceita pela administração e não previstos no item 28.4.1 do edital, aplicar-se-á Suspensão Temporária de participar em licitação e impedimento de contratar com o Ministério Público do Estado do Pará, pelo período de até 02 (dois) anos, na seguinte graduação:

I. 1 (um) ano, nos casos de inexecução parcial não justificada e/ou não aceita pela Administração ou irregularidade na execução;

II. 2 (dois) anos, nos casos de inexecução total não justificada e/ou não aceita pela Administração.

13.5. DECLARAÇÃO DE INIDONEIDADE

13.5.1. No caso de inexecução do objeto que configure ilícito penal, será declarada a inidoneidade da Contratada para licitar e contratar com a Administração Pública Estadual, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade.

CLÁUSULA DÉCIMA QUARTA – DA RESCISÃO

14.1. O presente Contrato poderá ser rescindido:

14.1.1. Unilateralmente nos casos enumerados nos incisos I a XII e XVII, do Art. 78 da Lei nº. 8.666/93;

14.1.2. Amigavelmente, por acordo entre as partes, reduzida a termo no processo da Licitação;

14.1.3. Judicialmente, nos termos da Legislação Processual.

14.1.4. No caso de rescisão Contratual, devidamente justificada nos autos do Processo, terá o contratado o prazo de 05 (cinco) dias úteis, contados da notificação, para apresentar o contraditório e a ampla defesa.

14.2. A inexecução total ou parcial do contrato enseja a sua rescisão, com as consequências contratuais e as previstas em lei ou regulamento

CLÁUSULA DÉCIMA QUINTA – DA FISCALIZAÇÃO

15.1. Será designado servidor para representar a Administração no exercício do dever de acompanhar e fiscalizar a execução do presente contrato, nos termos do art. 67 da Lei nº 8.666/93.

CLÁUSULA DÉCIMA SEXTA - DA PUBLICAÇÃO

16.1. A publicação do presente Instrumento em extrato, no Diário Oficial do Estado, ficará a cargo do Contratante, no prazo e forma disposto na legislação pertinente.

CLÁUSULA DÉCIMA SÉTIMA - DO FORO

17.1. Fica eleito o foro da Justiça Estadual do Pará, Comarca de Belém, Capital do Estado do Pará, para dirimir quaisquer questões oriundas do presente Contrato.

E por estarem justos, contratados e de comum acordo, assinam o presente em duas vias de igual teor e forma, que declaram haver lido, na presença de duas testemunhas, para que possa produzir seus efeitos legais.

Belém-Pa, de de 2021

MINISTÉRIO PÚBLICO DO ESTADO DO PARÁ
Contratante

XX
Contratada

Testemunhas:

1.

2.

RG:

RG:.....

ANEXO IV

DECLARAÇÃO DE CUMPRIMENTO DA RESOLUÇÃO N.º 37/2009-CNMP

Objeto da contratação:

A empresa _____, inscrita no CNPJ sob o nº _____, por intermédio de seu representante legal, Sr(a) _____, portador(a) da Carteira de Identidade n.º _____ e do CPF n.º _____.

DECLARA que não se enquadra em nenhum dos impedimentos previstos art. 3º da Resolução nº 037/2009-CNMP (alterado pela **Resolução nº 172/2017-CNMP**), onde prevê que é **VEDADA** “a contratação, independentemente da modalidade de licitação, de pessoa jurídica que tenha em seu quadro societário cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade até o terceiro grau, inclusive, dos membros ocupantes de cargos de direção ou no exercício de funções administrativas, assim como de servidores ocupantes de cargos de direção, chefia e assessoramento vinculados direta ou indiretamente às unidades situadas na linha hierárquica da área encarregada da licitação”.

A vedação, conforme o §1º, “não se aplica às hipóteses nas quais a contratação seja realizada por ramo do Ministério Público diverso daquele ao qual pertence o membro ou servidor gerador da incompatibilidade” e, de acordo com o §2º, “se estende às contratações cujo procedimento licitatório tenha sido deflagrado quando os membros e servidores geradores de incompatibilidade estavam no exercício dos respectivos cargos e funções, assim como às licitações iniciadas até 6 (seis) meses após a desincompatibilização”.

DECLARA, ainda, estar ciente das **SANÇÕES** que lhe poderão ser impostas, conforme disposto no respectivo Edital e no art. 299 do Código Penal, na hipótese de falsidade da presente declaração.

Belém-Pa, _____ de _____ de 2021.

Assinatura do Representante legal