# EDITAL PREGÃO ELETRÔNICO Nº 06/2021
## SECRETARIA DE ESTADO DA EDUCAÇÃO - SEDUC/PI
## Processo Administrativo n. 00011.001163-2020-32

Torna-se público, para conhecimento dos interessados, que a **SECRETARIA DE ESTADO DA EDUCAÇÃO - SEDUC/PI**, por meio da **Gerência de Licitação - GECOPELIC,** sediada na Av. Pedro Freitas, S/N, Centro Administrativo, Blocos D e F, CEP 64.018-900, realizará licitação do tipo **menor preço por lote grupo,** nos termos da Lei nº 10.520/2002, da Lei nº 8.248/1991, da Lei nº 9.279/1996, da Lei nº 9.742/1997, da Lei nº 9.610/1998; da Lei nº 10.176/2001, da Lei nº 12.305/2010, da Lei Estadual nº 6.301/2013, da Lei Estadual nº 6.735/2015, da Lei Estadual nº 6.947/2017, do Decreto Federal nº 7.174/2010, do Decreto Federal nº 7.746/2012, do Decreto Federal nº 9.507/2018, do Decreto Federal nº 10.024/2019, do Decreto Estadual nº 11.346/2004, Decreto Estadual nº 14.483/2011, da Instrução Normativa SLTI/MPOG nº 01, de 19 de janeiro de 2010, das Instruções Normativas SEGES/MP nº 05, de 26 de maio de 2017 e nº 03, de 26 de abril de 2018 e da Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019, da Lei Complementar n° 123/2006, do Decreto Federal n. 8.538/2015 e o do Decreto Estadual n. 16.212/2015, aplicando-se, subsidiariamente, a Lei nº 8.666/1993 e as exigências estabelecidas neste Edital.

Data início de Acolhimento: 04/03/2021

Horário: 08h00min

Data Abertura de propostas: 16/03/2021

Horário: 10h00min

Data Rodada de Lances: 16/03/2021

Horário: 10h00min

Local: Portal de Compras do Governo Federal – www.comprasgovernamentais.gov.br (UASG: 925478).

## 1. DO OBJETO

1.1 O objeto da presente licitação é a escolha da proposta mais vantajosa para a **Contratação de empresa para o fornecimento de renovação com upgrade tecnológico de solução integrada de Firewall Next Generation**, conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

1.2. A licitação será realizada em **grupo único,** formados por **16 (dezesseis)**

**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. Cada serviço ou produto do lote deverá estar discriminado em itens separados nas propostas de preços, de modo a permitir a identificação do seu preço individual na composição do preço global, e a eventual incidência sobre cada item das margens de preferência para produtos e serviços que atendam às Normas Técnicas Brasileiras – NTB.

## 2. DOS RECURSOS ORÇAMENTÁRIOS

2.1. As despesas para atender a esta licitação estão programadas em dotação orçamentária própria, prevista no orçamento da SEDUC/PI, para o exercício de 2020, na classificação abaixo:

Gestão/Unidade: 140102

Fonte: Tesouro Estadual (000025 - Precatórios do FUNDEF)

Programa de Trabalho: 12368021956

Elemento de Despesa: 3.3.90.39 / 4.4.90.52

PI: 1956

## 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, assumir 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 da senha, 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;

4.2. 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 insolvência, 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).

4.3. Nos termos do art. 5º do Decreto nº 9.507, de 2018, é vedada a contratação de pessoa jurídica na qual haja administrador ou sócio com poder de direção, familiar de:

a) detentor de cargo em comissão ou função de confiança que atue na área responsável pela demanda ou contratação; ou

b) de autoridade hierarquicamente superior no âmbito do órgão contratante.

4.3.1. Para os fins do disposto neste item, considera-se familiar o cônjuge, o companheiro ou o parente em linha reta ou colateral, por consanguinidade ou afinidade, até o terceiro grau (Súmula Vinculante/STF nº 13, art. 5º, inciso V, da Lei nº 12.813, de 16 de maio de 2013 e art. 2º, inciso III, do Decreto n.º 7.203, de 04 de junho de 2010);

4.4. Nos termos do art. 7° do Decreto n° 7.203, de 2010, é vedada, ainda, a utilização, na execução dos serviços contratados, de empregado da futura Contratada que seja familiar de agente público ocupante de cargo em comissão ou função de confiança neste órgão contratante.

4.5. Como condição para participação no Pregão, o licitante assinalará “sim” ou “não” em campo próprio do sistema eletrônico, relativo às seguintes declarações:

4.5.1. que cumpre os requisitos estabelecidos no artigo 3° da Lei Complementar nº 123, de 2006, estando apto a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49.

4.5.1.1. nos itens exclusivos para participação de microempresas e empresas de pequeno porte, a assinalação do campo “não” impedirá o prosseguimento no certame;

4.5.1.2. 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 ou sociedade cooperativa.

4.5.2. que está ciente e concorda com as condições contidas no Edital e seus anexos;

4.5.3. que cumpre plenamente os requisitos de habilitação definidos no Edital e que a proposta apresentada está em conformidade com as exigências editalícias;

4.5.4. que inexistem fatos impeditivos para sua habilitação no certame, ciente da obrigatoriedade de declarar ocorrências posteriores;

4.5.5. 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 7°, XXXIII, da Constituição;

4.5.6. que a proposta foi elaborada de forma independente, nos termos da Instrução Normativa SLTI/MP nº 2, de 16 de setembro de 2009.

4.5.7. 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;

4.5.8. 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.

4.5.9. que cumpre os requisitos do Decreto n. 7.174, de 2010, estando apto a usufruir dos critérios de preferência.

4.5.9.1. a assinalação do campo “não” apenas produzirá o efeito de o licitante não ter direito ao tratamento favorecido previsto no Decreto nº 7.174, de 2010.

4.6. 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 a abertura da sessão pública, quando, então, encerrar-se-á automaticamente a etapa de envio desse documento.

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. PREENCHIMENTO DA PROPOSTA

6.1. O licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, dos seguintes campos:

6.1.1. Valor total do lote;

6.1.2. Descrição do objeto, contendo as informações similares à especificação do Termo de Referência.

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 na prestação dos serviços, apurados mediante o preenchimento do modelo de Planilha de Custos e Formação de Preços, conforme anexo deste Edital.

6.3.1. A Contratada deverá arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, tais como os valores providos com o quantitativo de vale transporte, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da licitação, exceto quando ocorrer algum dos eventos arrolados nos incisos do §1° do artigo 57 da Lei n° 8.666, de 1993;

6.3.2. Caso o eventual equívoco no dimensionamento dos quantitativos se revele superior às necessidades da contratante, a Administração deverá efetuar o pagamento seguindo estritamente as regras contratuais de faturamento dos serviços demandados e executados, concomitantemente com a realização, se necessário e cabível, de adequação contratual do quantitativo necessário, com base na alínea "b" do inciso I do art. 65 da Lei n. 8.666/93 e nos termos do art. 63, §2° da IN SEGES/MPDG n. 5/2017.

6.4. A empresa é a única responsável pela cotação correta dos encargos tributários. Em caso de erro ou cotação incompatível com o regime tributário a que se submete, serão adotadas as orientações a seguir:

6.4.1. cotação de percentual menor que o adequado: o percentual será mantido durante toda a execução contratual;

6.4.2. cotação de percentual maior que o adequado: o excesso será suprimido, unilateralmente, da planilha e haverá glosa, quando do pagamento, e/ou redução, quando da repactuação, para fins de total ressarcimento do débito.

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

contratada apresentar ao pregoeiro ou à fiscalização, a qualquer tempo, comprovação da adequação dos recolhimentos, para os fins do previsto no subitem anterior.

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

6.7. A apresentação das propostas implica obrigatoriedade do cumprimento das disposições nelas contidas, em conformidade com o que dispõe o Termo de Referência, assumindo o proponente o compromisso de executar os serviços nos seus termos, bem como de fornecer os materiais, equipamentos, ferramentas e utensílios necessários, em quantidades e qualidades adequadas à perfeita execução contratual, promovendo, quando requerido, sua substituição.

6.8. 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.

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

6.10. Os licitantes devem respeitar os preços máximos estabelecidos nas normas de regência de contratações públicas federais, quando participarem de licitações públicas;

6.10.1. O descumprimento das regras supramencionadas pela Administração por parte dos contratados pode ensejar a responsabilização pelo Tribunal de Contas da União e, após o devido processo legal, gerar as seguintes consequências: assinatura de prazo para a adoção das medidas necessárias ao exato cumprimento da lei, nos termos do art. 71, inciso IX, da Constituição; ou condenação dos agentes públicos responsáveis e da empresa contratada ao pagamento dos prejuízos ao erário, caso verificada a ocorrência de superfaturamento por sobrepreço na execução do contrato.

## 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, ilegalidades, ou não apresentem as especificações 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 de sistema eletrônico, sendo imediatamente informados do seu recebimento e do valor consignado no registro.

7.5.1. O lance deverá ser ofertado pelo **valor total do lote**.

7.6. Os licitantes poderão oferecer lances sucessivos, observando o horário fixado para abertura da sessão e as regras estabelecidas no Edital.

7.7. O licitante somente poderá oferecer lance de valor inferior ou percentual de desconto superior ao último por ele ofertado e registrado pelo sistema.

7.8. O intervalo mínimo de diferença de valores ou percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser de **R$ 10,00 (dez reais).**

7.9. Será adotado para o envio de lances no pregão eletrônico o **modo de disputa "aberto e fechado"**, em que os licitantes apresentarão lances públicos e sucessivos, com lance final e fechado.

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

7.11 Encerrado o prazo previsto no item anterior, o sistema abrirá oportunidade para que o autor da oferta de valor mais baixo e os das ofertas com preços até dez por cento superiores àquela possam ofertar um lance final e fechado em até cinco minutos, o que será sigiloso até o encerramento deste prazo.

7.11.1 Não havendo, pelo menos, três ofertas nas condições definidas neste item poderão os autores dos melhores lances subsequentes, na ordem de classificação, até o máximo de três, oferecer um lance final e fechado até cinco minutos, o qual será sigiloso até o encerramento deste prazo.

7.12 Após o término dos prazos estabelecidos nos itens anteriores, o sistema ordenará os lances segundo a ordem crescente de valores.

7.12.1 Não havendo lance final fechado e classificado na forma estabelecida nos itens anteriores, haverá o reinício da etapa fechada para que os demais licitantes, até no máximo de três, na ordem de classificação, possam ofertar um lance final e fechado em até cinco minutos, o qual será sigiloso até o encerramento deste prazo, observando-se, após, o item anterior.

7.13 Poderá o pregoeiro, auxiliado pela equipe de apoio, justificadamente, admitir o reinício da etapa fechada, caso nenhum licitante classificado na etapa de lance fechado atender as exigências de habilitação

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

7.15. Durante o transcurso da sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado, vedada a identificação do licitante.

7.16. 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.

7.17. Quando a desconexão do sistema eletrônico para o pregoeiro persistir por tempos superior a dez minutos, a sessão pública será suspensa e reiniciada

somente após decorridas vinte e quatro horas após a comunicação do fato aos participantes no sítio eletrônico utilizado para divulgação.

7.18. O Critério de julgamento adotado será o **menor preço global por grupo único**, conforme definido neste Edital e seus anexos.

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

7.20. 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.

7.21. 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.

7.22. 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.

7.23. 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.

7.24. 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.

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

7.26. 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:

7.26.1. prestados por empresas brasileiras;

7.26.2. prestados por empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País;

7.26.3. 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.

7.27. Persistindo o empate, a proposta vencedora será sorteada pelo sistema eletrônico dentre as propostas ou os lances empatados.

7.28. 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 prevista deste Edital.

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

7.28.2. O pregoeiro solicitará ao licitante melhor classificado que, no prazo de **24 (vinte e quatro) 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.

7.29. Após a negociação do preço, o Pregoeiro iniciará a fase de aceitação e julgamento da proposta.

7.30. Será assegurado o direito de preferência previsto no seu artigo 3º, conforme procedimento estabelecido nos artigos 5° e 8° do Decreto n° 7.174, de 2010.

7.30.1. As licitantes qualificadas como microempresas ou empresas de pequeno porte que fizerem jus ao direito de preferência previsto no Decreto nº 7.174, de 2010, terão prioridade no exercício desse benefício em relação às médias e às grandes empresas na mesma situação.

## 8. DA ACEITABILIDADE DA PROPOSTA VENCEDORA.

8.1. Encerrada a etapa de negociação, o pregoeiro examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade de 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 nº 10.024/2019.

8.2. A análise da exequibilidade da proposta de preços deverá ser realizada com o auxílio da Planilha de Custos e Formação de Preços, a ser preenchida pelo licitante em relação à sua proposta final, conforme anexo deste Edital.

8.3. A Planilha de Custos e Formação de Preços deverá ser encaminhada pelo licitante exclusivamente via sistema, no prazo de **02 (duas horas)**, contado da solicitação do Pregoeiro, com os respectivos valores adequados ao lance vencedor e será analisada pelo Pregoeiro no momento da aceitação do lance vencedor.

8.4. A inexequibilidade dos valores referentes a itens isolados da Planilha de Custos e Formação de Preços não caracteriza motivo suficiente para a desclassificação da proposta, desde que não contrariem exigências legais.

8.5. Será desclassificada a proposta ou o lance vencedor, nos termos do item 9.1 do Anexo VII-A da In SEGES/MPDG n. 5/2017, que:

8.5.1. não estiver em conformidade com os requisitos estabelecidos neste edital;

8.5.2. contenha vício insanável ou ilegalidade;

8.5.3. não apresente as especificações técnicas exigidas pelo Termo de Referência;

8.5.4. apresentar preço final superior ao preço máximo fixado (Acórdão nº 1455/2018-TCU – Plenário), desconto menor do que o mínimo exigido, ou que apresentar preço manifestamente inexequível.

8.5.4.1. Quando o licitante não conseguir comprovar que possui ou possuirá recursos suficientes para executar a contento o objeto, será considerada inexequível a proposta de preços ou menor lance que:

8.5.4.1.1. for insuficiente para a cobertura dos custos da contratação, 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.

8.5.4.2. apresentar um ou mais valores da planilha de custo que sejam inferiores àqueles fixados em instrumentos de caráter normativo obrigatório, tais como leis, medidas provisórias e convenções coletivas de trabalho vigentes.

8.6. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, na forma do § 3° do artigo 43 da Lei n° 8.666, de 1993 e a exemplo das enumeradas no item 9.4 do Anexo VII-A da IN SEGES/MPDG N. 5, de 2017, para que a empresa comprove a exequibilidade da proposta.

8.7. Quando o licitante apresentar preço final inferior a 30% (trinta por cento) da média dos preços ofertados para o mesmo item, e a inexequibilidade da proposta não for flagrante e evidente pela análise da planilha de custos, não sendo possível a sua imediata desclassificação, será obrigatória a realização de diligências para aferir a legalidade e exequibilidade da proposta.

8.8. Qualquer interessado poderá requerer que se realizem diligências para aferir a exequibilidade e a legalidade das propostas, devendo apresentar as provas ou os indícios que fundamentam a suspeita.

8.8.1. Na hipótese de necessidade de suspensão de sessão pública para a realização de diligências, com vista 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.

8.9. O Pregoeiro poderá convocar o licitante para enviar documento digital complementar, por meio de funcionalidade disponível no sistema, no prazo de **02 (duas horas)**, sob pena de não aceitação da proposta.

8.9.1. É facultado ao pregoeiro prorrogar o prazo estabelecido, a partir de solicitação fundamentada feita no chat pelo licitante, antes de findo o prazo

8.9.2. Dentre os documentos passíveis de solicitação pelo Pregoeiro, destacam-se as planilhas de custo readequadas com o valor final ofertado.

8.10. Todos os dados informados pelo licitante em sua planilha deverão refletir com fidelidade os custos especificados e a margem de lucro pretendida.

8.11. O Pregoeiro analisará a compatibilidade dos preços unitários apresentados na Planilha de Custos e Formação de Preços com aqueles praticados no mercado em relação aos insumos e também quanto aos salários das categorias envolvidas na contratação;

8.12. Erros no preenchimento da planilha não constituem motivo para a desclassificação da proposta. A planilha poderá ser ajustada pelo licitante, no prazo indicado pelo Pregoeiro, desde que não haja majoração do preço.

8.12.1.O ajuste de que trata este dispositivo se limita a sanar erros ou falhas que não alterem a substância das propostas.

8.12.2. Considera-se erro no preenchimento da planilha passível de correção a indicação de recolhimento de impostos e contribuições na forma do Simples Nacional, quando não cabível esse regime.

8.13. 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.

8.14. Se a proposta ou lance vencedor for desclassificado, o Pregoeiro examinará a proposta ou lance subsequente, e, assim sucessivamente, na ordem de classificação.

8.15. Havendo necessidade, o Pregoeiro suspenderá a sessão, informando no “chat” a nova data e horário para a sua continuidade.

8.16. 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. 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, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

a) SICAF;

b) Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS, mantido pela Controladoria-Geral da União (www.portaldatransparencia.gov.br/ceis);

c) Cadastro Nacional de Condenações Cíveis por Atos de Improbidade Administrativa, mantido pelo Conselho Nacional de Justiça (www.cnj.jus.br/improbidade_adm/consultar_requerido.php).

d) Lista de Inidôneos e o Cadastro Integrado de Condenações por Ilícitos Administrativos - CADICON, mantidos pelo Tribunal de Contas da União - TCU.

9.1.1 Para a consulta de licitantes pessoa jurídica poderá haver a substituição das consultas das alíneas “b”, “c” e “d” acima pela Consulta Consolidada de Pessoa Jurídica do TCU (https://certidoesapf.apps.tcu.gov.br/)

9.1.2 A consulta aos cadastros será realizada em nome da empresa licitante e também de seu sócio majoritário, por força do artigo 12 da Lei n° 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.

9.1.2.1 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.

9.1.2.1.1 A tentativa de burla será verificada por meio dos vínculos

societários, linhas de fornecimento similares, dentre outros.

9.1.2.1.2 O licitante será convocado para manifestação previamente à sua desclassificação.

9.1.3 Constatada a existência de sanção, o Pregoeiro reputará o licitante inabilitado, por falta de condição de participação.

9.1.4 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 à qualificação econômica financeira, 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 **02 (duas) horas**, sob pena de inabilitação.

9.4 Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante a apresentação dos documentos originais não-digitais quando houver dúvida em relação à integridade do documento digital. Não serão aceitos documentos de habilitação com indicação de CNPJ/CPF diferentes, salvo aqueles legalmente permitidos.

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 diferentes números de documentos pertinentes ao CND e ao CRF/FGTS, quando for comprovada a centralização do recolhimento dessas contribuições.

9.7 Ressalvado o disposto do item 5.3, os licitantes deverão encaminhar, nos termos deste Edital, a documentação nos itens a seguir, para fins de habilitação.

9.8 **Habilitação jurídica:**

9.8.1 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;

9.8.2 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;

9.8.3 inscrição no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz, no caso de ser o participante sucursal, filial ou agência;

9.8.4 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;

9.8.5 decreto de autorização, em se tratando de sociedade empresária estrangeira em funcionamento no País;

9.8.6 No caso de empresa ou sociedade estrangeira em funcionamento no País, o Decreto de autorização e o ato de registro ou autorização para funcionamento expedido pelo órgão competente, quando a atividade assim o exigir;

9.8.6.1. O documento de habilitação referido neste subitem deverá explicitar o objeto social, que deverá ser compatível com o objeto desta licitação, segundo a tabela de classificação do CNAE, a sede da licitante e os responsáveis por sua administração que tenham poderes para assinar os documentos pela licitante;

9.8.7 Os documentos acima deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

**9.9 Regularidade fiscal e trabalhista:**

9.9.1 prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;

9.9.2 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.

9.9.3 prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

9.9.4 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;

9.9.5 prova de inscrição no cadastro de contribuintes estadual, relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

9.9.6 prova de regularidade com a Fazenda Estadual do domicílio e sede do licitante, relativa à atividade em cujo exercício contrata ou concorre;

9.9.7 caso o licitante seja considerado isento dos tributos estaduais relacionados ao objeto licitatório, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda Estadual do seu domicílio ou sede, ou outra equivalente, na forma da lei;

9.9.8 Quando se tratar da subcontratação prevista no art. 48, II, da Lei Complementar n. 123, de 2006, a licitante melhor classificada deverá, também, apresentar a documentação de regularidade fiscal e trabalhista 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.

**9.10 Qualificação Econômico-Financeira:**

9.10.1 Certidão negativa de falência expedida pelo distribuidor da sede do licitante;

9.10.2 Balanço patrimonial e demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, que comprovem a boa situação financeira da empresa, vedada a sua substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais quando encerrado há mais de 3 (três) meses da data de apresentação da proposta;

9.10.2.1 no caso de empresa constituída no exercício social vigente, admite-se a apresentação de balanço patrimonial e demonstrações contábeis referentes ao período de existência da sociedade;

9.10.2.2 é admissível o balanço intermediário, se decorrer de lei ou contrato/estatuto social.

9.10.3 Comprovação da boa situação financeira da empresa mediante obtenção de índices de Liquidez Geral (LG), Solvência Gral (SG) e Liquidez Corrente (LC), superiores a 1 (um), obtidos pela aplicação das seguintes fórmulas:

| | |
|---|---|
| LG = | Ativo Circulante + Realizável a Longo Prazo |
| | Passivo Circulante + Passivo Não Circulante |

| | |
|---|---|
| SG = | Ativo Total |
| | Passivo Circulante + Passivo Não Circulante |

| | |
|---|---|
| LC = | Ativo Circulante |
| | Passivo Circulante |

9.10.4 As empresas, que apresentarem resultado inferior ou igual a 1 (um)

em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), deverão comprovar patrimônio líquido de 10% (dez por cento) do valor total estimado da contratação ou do item pertinente.

**9.11 Qualificação Técnica:**

9.11.1. Comprovação de aptidão para a prestação dos serviços em características, quantidades e prazos compatíveis com o objeto desta licitação, ou com o item pertinente, mediante a apresentação de atestado(s) fornecido(s) por pessoas jurídicas de direito público ou privado.

9.11.1.1. Para fins da comprovação de que trata este subitem, os atestados deverão dizer respeito a serviços executados com as seguintes características mínimas:

9.11.1.1.1 Nome do contratado e do contratante;

9.11.1.1.2 Nome completo e telefone de contato do responsável pelo contrato na contratante (responsável pelo atestado);

9.11.1.1.3 Identificação do contrato (tipo ou natureza do serviço);

9.11.1.1.4 Vigência do contrato;

9.11.1.1.5 Local da execução dos serviços;

9.11.1.1.6 Descrição dos serviços executados e parecer do contratante quanto à qualidade do serviço prestado.

9.11.1.2. Por se tratar de serviço que requer de seu executor conhecimentos técnicos especializados em face do grau de complexidade envolvida, o licitante vencedor deverá apresentar atestado(s), declaração(ões) ou certidão(ões) de capacidade técnica, fornecido por pessoa jurídica, de direito público ou privado, que comprove a prestação de suporte e manutenção de solução de **Firewall Next Generation da fabricante BlockBit**, de forma satisfatória, pertinente e compatível com o objeto do Termo de Referência.

9.11.1.2.1 As empresas deverão comprovar, ainda, a qualificação técnica, por meio de comprovação de aptidão para a prestação dos serviços em características compatíveis com o objeto desta licitação, ou com o item pertinente, mediante a apresentação de atestados fornecidos por pessoas jurídicas de direito público ou privado.

9.11.1.2.1.1 Entende-se como compatível com objeto desta licitação a prestação de serviço de manutenção e suporte a solução de **Firewall Next Generation da fabricante BlockBit**, englobando o suporte ao software e ao hardware.

9.11.1.3. **Requisitos de Experiência Profissional:**

9.11.1.3.1 A empresa deverá possuir no mínimo 01 (um) técnico certificado pelo fabricante da solução;

9.11.1.3.2 A exigência se faz necessária tendo em vista que a solução afeta diretamente a segurança da informação e a disponibilidade de todos os sites, sistemas e aplicações hospedadas no Centro de Dados da SEDUC disponíveis na Internet. Trata-se de um serviço que é extremamente crítico para a SEDUC e não são admissíveis falhas no processo de suporte. A exigência de expertise do licitante vencedor visa minimizar os riscos relacionados a

sustentação dos serviços;

9.11.1.3.3 Na ocasião da assinatura do contrato o licitante vencedor deverá entregar cópias digitalizadas dos certificados.

9.11.1.4. **Requisitos de Segurança da Informação:**

9.11.1.4.1 Manter sigilo de todos os dados ou informações da SEDUC conforme o Termo de Confidencialidade **(ANEXO V)**, obtidas em função da execução do objeto, sujeitando-se às cominações legais, nos termos da Lei 4.595 de 31.12.1964 e da Lei 13.709 de 14.08.2018 e demais leis correlatas.

9.11.1.4.2 O representante da Contratante deverá comunicar à Contratada por escrito, quanto à Política de Segurança da Informação da Secretaria de Estado da Educação e suas normas complementares, para ciência e para que se responsabilize por todas as providências e deveres estabelecidos.

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

9.11.3. Somente serão aceitos atestados expedidos após a conclusão do contrato ou se decorrido, pelo menos, um ano do início de sua execução, exceto se firmado para ser executado em prazo inferior, conforme item 10.8 da IN SEGES/MPDG n. 5, de 2017.

9.11.4. 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 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.

9.11.5. 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.

9.11.5.1 A exigência se faz necessária tendo em vista que a solução afeta diretamente a segurança da informação e a disponibilidade de todos os sites, sistemas e aplicações hospedadas no Centro de Dados da SEDUC disponíveis na Internet. Trata-se de um serviço que é extremamente crítico para a SEDUC e não são admissíveis falhas no processo de suporte. A exigência de expertise do licitante vencedor visa minimizar os riscos relacionados a sustentação dos serviços e a expertise em soluções de outros fabricantes não garante a expertise na referida solução, podendo colocar em risco desnecessário a continuidade na prestação do serviço de segurança provido pela solução.

9.11.6. As empresas, cadastradas ou não no SICAF, deverão apresentar atestado de vistoria assinado pelo servidor responsável, caso exigida no Termo de Referência.

9.11.6.1 O atestado de vistoria poderá ser substituído por declaração emitida pelo licitante em que conste, alternativamente, ou que conhece as condições locais para execução do objeto; ou que tem pleno conhecimento das condições e peculiaridades inerentes à natureza do

trabalho, assume total responsabilidade por este fato e não utilizará deste para quaisquer questionamentos futuros que ensejem desavenças técnicas ou financeiras com a contratante.

9.12. 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.

9.13. 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.

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

9.14. Caso a proposta mais vantajosa seja ofertada por microempresa, 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 05 (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.

9.15. 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.

9.16. 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.

9.17. 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.

9.18. 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.

9.19. Constatado o atendimento às exigências de habilitação fixadas no Edital, o licitante será declarado vencedor.

## 10. DO ENCAMINHAMENTO DA PROPOSTA VENCEDORA

10.1 A proposta final do licitante declarado vencedor deverá ser encaminhada no prazo de **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.

10.1.2 apresentar a planilha de custos e formação de preços, devidamente ajustada ao lance vencedor, em conformidade com o modelo anexo a este instrumento convocatório.

10.1.3 conter a indicação do banco, número da conta e agência do licitante vencedor, para fins de pagamento.

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 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.

## 11. DOS RECURSOS

11.1 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 01 (uma) horas, para que qualquer licitante manifeste a intenção de recorrer, de forma motivada, isto é, indicando contra qual(is) decisão(ões) pretende recorrer e por quais motivos, em campo próprio do sistema.

11.2 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.

11.2.1 Nesse momento o Pregoeiro não adentrará no mérito recursal, mas apenas verificará as condições de admissibilidade do recurso.

11.2.2 A falta de manifestação motivada do licitante quanto à intenção de recorrer importará a decadência desse direito.

11.2.3 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.

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

11.4 Os autos do processo permanecerão com vista franqueada aos interessados, no endereço constante neste Edital.

## 12. DA REABERTURA DA SESSÃO PÚBLICA

12.1 A sessão pública poderá ser reaberta:

12.1.2 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, 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, de acordo com a fase do procedimento licitatório.

12.2.2 A convocação feita por e-mail dar-se-á de acordo com os dados contidos no SICAF, sendo responsabilidade do licitante manter seus dados cadastrais atualizados.

## 13. DA ADJUDICAÇÃO E HOMOLOGAÇÃO

13.1 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.

13.2 Após a fase recursal, constatada a regularidade dos atos praticados, a autoridade competente homologará o procedimento licitatório.

## 14. DA GARANTIA DE EXECUÇÃO

14.1 Será exigida a prestação de garantia na presente contratação, conforme regras constantes do Termo de Referência.

## 15. DO TERMO DE CONTRATO OU INSTRUMENTO EQUIVALENTE

15.1 Após a homologação da licitação, em sendo realizada a contratação, será firmado Termo de Contrato ou emitido instrumento equivalente.

15.2 O adjudicatário terá o prazo de 05 (cinco) 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.

15.2.1 Alternativamente à convocação para comparecer perante o órgão ou entidade para a assinatura do Termo de Contrato, a Administração poderá encaminhá-lo para assinatura, mediante correspondência postal com aviso de recebimento (AR) ou meio eletrônico, para que seja assinado e devolvido no prazo de 05 (cinco) dias úteis, a contar da data de seu recebimento.

15.2.2 O prazo previsto no subitem anterior poderá ser prorrogado, por igual período, por solicitação justificada do adjudicatário e aceita pela Administração.

15.3 O Aceite da Nota de Empenho ou do instrumento equivalente, emitida à empresa adjudicada, implica no reconhecimento de que:

15.3.1 Referida Nota está substituindo o contrato, aplicando-se à relação de negócios ali estabelecida as disposições da Lei nº 8.666, de 1993;

15.3.2 A contratada se vincula à sua proposta e às previsões contidas no edital e seus anexos;

15.3.3 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.

15.4 O **prazo de vigência da contratação é de 48 (quarenta e oito) meses** conforme previsão no instrumento contratual.

15.5 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.

15.5.1 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.

15.5.2 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.

15.6 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.

15.7 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.

## 16. DO REAJUSTAMENTO EM SENTIDO GERAL

16.1 As regras acerca do reajustamento em sentido geral do valor contratual são as estabelecidas no item 17.1.1. do Termo de Referência, anexo a este Edital.

## 17. DO RECEBIMENTO DO OBJETO E DA FISCALIZAÇÃO

17.1 Os critérios de recebimento e aceitação do objeto e de fiscalização estão previstos no Termo de Referência.

## 18. DAS OBRIGAÇÕES DA CONTRATANTE E DA CONTRATADA

18.1 As obrigações da Contratante e da Contratada são as estabelecidas no Termo de Referência.

## 19. DO PAGAMENTO

19.1 As regras acerca do pagamento são as estabelecidas no Termo de Referência, anexo a este Edital.

## 20. DAS SANÇÕES ADMINISTRATIVAS.

20.1 Comete infração administrativa, nos termos da Lei nº 10.520, de 2002, o licitante/adjudicatário que:

20.1.1 não assinar o termo de contrato ou aceitar/retirar o instrumento equivalente, quando convocado dentro do prazo de validade da proposta;

20.1.2 não assinar a ata de registro de preços, quando cabível;

20.1.3 apresentar documentação falsa;

20.1.4 deixar de entregar os documentos exigidos no certame;

20.1.5 ensejar o retardamento da execução do objeto;

20.1.6 não mantiver a proposta;

20.1.7 cometer fraude fiscal;

20.1.8 comportar-se de modo inidôneo;

20.2 As sanções do item acima também se aplicam aos integrantes do cadastro de reserva, em pregão para registro de preços que, convocados, não honrarem o compromisso assumido injustificadamente.

20.3 Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os licitantes, em qualquer momento da licitação, mesmo após o encerramento da fase de lances.

20.4 O licitante/adjudicatário que cometer qualquer das infrações discriminadas nos subitens anteriores ficará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

20.4.1 Advertência por faltas leves, assim entendidas como aquelas que não acarretarem prejuízos significativos ao objeto da contratação;

20.4.2 Multa de 10% (dez por cento) sobre o valor estimado do(s) item(s) prejudicado(s) pela conduta do licitante;

20.4.3 Suspensão de licitar e impedimento de contratar com o órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente, pelo prazo de até dois anos;

20.4.4 Impedimento de licitar e de contratar com a União e descredenciamento no SICAF, pelo prazo de até cinco anos;

20.4.5 Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a Contratada ressarcir a Contratante pelos prejuízos causados;

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

20.6 Se, durante o processo de aplicação de penalidade, se 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.

20.7 A apuração e o julgamento das demais infrações administrativas não consideradas como ato lesivo à Administração Pública nacional ou estrangeira nos termos da Lei nº 12.846, de 1º de agosto de 2013, seguirão seu rito normal na unidade administrativa.

20.8 O processamento do PAR não interfere no seguimento regular dos processos administrativos específicos para apuração da ocorrência de danos e prejuízos à Administração Pública Federal resultantes de ato lesivo cometido por pessoa jurídica, com ou sem a participação de agente público.

20.9 Caso o valor da multa não seja suficiente para cobrir os prejuízos causados pela conduta do licitante, a União ou Entidade poderá cobrar o valor remanescente judicialmente, conforme artigo 419 do Código Civil.

20.10 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.

20.11 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.

20.12 As penalidades serão obrigatoriamente registradas no SICAF.

20.13 As sanções por atos praticados no decorrer da contratação estão previstas no Termo de Referência.

## 21. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

21.1 Até 03 (três) dias úteis antes da data designada para a abertura da sessão pública, qualquer pessoa poderá impugnar este Edital.

21.2 O pedido de impugnação deverá ser enviado ao endereço eletrônico pregaoseducpi@gmail.com e também deverá ser protocolado por meio do Sistema Eletrônico de Informação (SEI), em substituição à abertura de novos processos físicos; Segue orientações:

a) Os particulares (pessoa física ou pessoa jurídica) que desejarem se utilizar

do direito de petição, deverão apresentar documentos e/ou requerimentos em formato PDF através de mídia digital (CD ou pen-drive), que será utilizada pelo servidor no momento da protocolização e em seguida devolvida ao interessado juntamente com o número do processo que foi gerado;

b) Caso a documentação a ser protocolizada neste Órgão não exceda a 10 (dez) páginas, esta poderá ser recebida no seu formato original para conversão no formato PDF e registro do processo no SEI, sendo, posteriormente, devolvida ao interessado juntamente com o número do processo que foi gerado;

c) A Supervisão de Protocolo Geral deste Órgão disponibiliza o endereço eletrônico (protocologeral@seduc.pi.gov.br) para recebimento de documentos e/ou requerimentos em formato PDF, para abertura de processos no SEI, desde que possa ser confirmada a autenticidade do remetente/interessado;

d) As diligências e respostas que se fizerem necessárias nos processos administrativos previstos acima, serão formuladas, preferencialmente, através do SEI ou de endereço de e-mail, devendo o requerente/interessado fornecer o endereço correspondente no documento que dará início ao processo;

e) Quando houver impossibilidade técnica de digitalização de documentos, estes serão recebidos em sua forma original, sendo posteriormente registrados no SEI;

f) Fica vedada a abertura de processos no SEI utilizando-se de documentação ilegível.

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

21.4 Acolhida a impugnação, será definida e publicada nova data para a realização do certame.

21.5 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 endereço indicado no Edital.

21.6 O pregoeiro responderá aos pedidos de esclarecimentos no prazo de dois dias úteis, contados da data do recebimento do pedido e poderá requisitar subsídios formais aos responsáveis pela elaboração do edital e dos anexos

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

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

21.8 As respostas aos pedidos de esclarecimentos serão divulgadas pelo sistema e vincularão os participantes e a administração.

## 22. DAS DISPOSIÇÕES GERAIS

22.1 Da sessão pública do Pregão divulgar-se-á o resultado no sistema eletrônico.

22.2 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.

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

22.4 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.

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

22.6 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.

22.7 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.

22.8 O desatendimento de exigências formais não essenciais não importará o afastamento do licitante, desde que seja possível o aproveitamento do ato, observados os princípios da isonomia e do interesse público.

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

22.10 O Edital está disponibilizado, na íntegra, nos endereços eletrônicos www.seduc.pi.gov.br/licitacoes e www.tce.pi.gov/licitacao, sendo os autos do processo administrativo com vista franqueada aos interessados no endereço da SEDUC em horário e dias úteis.

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

22.11.1. ANEXO I - Termo de Referência;

22.11.2. ANEXO II – Minuta de Termo de Contrato;

22.11.3. ANEXO III – Modelo de Proposta de Preços;

22.11.4. ANEXO IV – Modelos de Declarações;

22.11.4. ANEXO V – Modelo de Termo de Confiabilidade.

Teresina(PI), 1º de março de 2021

Leovidio Neto

Gerente de Licitação

---

Documento assinado eletronicamente por **LEOVIDIO BEZERRA LIMA NETO - Matr.0171745-6**, **Gerente**, em 01/03/2021, às 11:28, conforme horário oficial de Brasília, com fundamento no Cap. III, Art. 14 do Decreto Estadual nº 18.142, de 28 de fevereiro de 2019.

**TERMO DE REFERÊNCIA**
**(Processo Administrativo n.°.....)**

## 1. DO OBJETO

**1.1.** Contratação de empresa para o fornecimento de renovação com upgrade tecnológico de solução integrada de Firewall NEXT GENERATION, conforme condições quantidades e exigências estabelecidas neste instrumento.

| **ITEM 1: RENOVAÇÃO BB 10** | | | | | | |
|---|---|---|---|---|---|---|
| **ITEM** | **PART NUMBER** | **DESCRIÇÃO** | **CATMAT CATSERV** | **QTDE** | **VALOR UNIT.** | **VALOR TOTAL** |
| 1.1 | BBHWUTM023 | Standard Software License - UTM Subscription - APL BB 10 - for 36 months | 27502 | 450 | R$ 5.539,32 | R$ 2.492.694,00 |
| 1.2 | BBSSR00289 | Suporte 14x6 - Banco de Horas Mensal - 3hrs - for 36 months | 27022 | 450 | R$ 4.865,00 | R$ 2.189.250,00 |
| **ITEM 2: RENOVAÇÃO BB 10000** | | | | | | |
| **ITEM** | **PART NUMBER** | **DESCRIÇÃO** | **CATMAT CATSERV** | **QTDE** | **VALOR UNIT.** | **VALOR TOTAL** |
| 2.1 | BBHWUTM054 | Standard Software License - UTM Subscription Advanced - APL BB 10000 - for 36 months | 27502 | 02 | R$ 127.919,51 | R$ 255.839,02 |
| 2.2 | BBSSR00289 | Suporte 14x6 - Banco de Horas Mensal - 3hrs - for 36 months | 27022 | 02 | R$ 4.865,00 | R$ 9.730,00 |
| **ITEM 3: AQUISIÇÃO BB 10** | | | | | | |
| **ITEM** | **PART NUMBER** | **DESCRIÇÃO** | **CATMAT CATSERV** | **QTDE** | **VALOR UNIT.** | **VALOR TOTAL** |
| 3.1 | BBHWUTM019 | Hardware Appliance APL UTM BB 10 | 150100 | 205 | R$ 3.665,00 | R$ 751.325,00 |
| 3.2 | BBHWUTM020 | Standard Software License - APL UTM BB 10 | 27502 | 205 | R$ 3.240,00 | R$ 664.200,00 |
| 3.3 | BBHWUTM023 | Standard Software License - UTM Subscription - APL BB 10 - for 36 months | 27502 | 205 | R$ 5.539,32 | R$ 1.135.560,60 |
| 3.4 | BBSSR00289 | Suporte 14x6 - Banco de Horas Mensal - 3hrs - for 36 months | 27022 | 205 | R$ 4.865,00 | R$ 997.325,00 |
| 3.5 | Instalação – 8 horas | Serviço de instalação | 26972 | 205 | R$ 1.632,50 | R$ 334.662,50 |
| **ITEM 4: AQUISIÇÃO BB 10 SPARE** | | | | | | |
| **ITEM** | **PART NUMBER** | **DESCRIÇÃO** | **CATMAT CATSERV** | **QTDE** | **VALOR UNIT.** | **VALOR TOTAL** |
| 4.1 | BBHWUTM024 | Hardware Appliance APL UTM BB 10 - Spare | 150100 | 35 | R$ 3.665,00 | R$ 128.275,00 |

| | | | | | | |
|---|---|---|---|---|---|---|
| 4.2 | BBHWUTM251 | Sistema Operacional Spare - APL UTM BB 10 | 27502 | 35 | R$ 1.065,00 | R$ 37.275,00 |
| **ITEM 5: AQUISIÇÃO BB 50** | | | | | | |
| **ITEM** | **PART NUMBER** | **DESCRIÇÃO** | **CATMAT CATSERV** | **QTDE** | **VALOR UNIT.** | **VALOR TOTAL** |
| 5.1 | BBHWUTM055 | Hardware Appliance APL UTM BB 50 | 150100 | 21 | R$ 4.809,79 | R$ 101.005,59 |
| 5.2 | BBHWUTM056 | Standard Software License - APL UTM BB 50 | 27502 | 21 | R$ 6.450,00 | R$ 135.450,00 |
| 5.3 | BBHWUTM059 | Standard Software License - UTM Subscription - APL BB 50 - for 36 months | 27502 | 21 | R$ 9.750,00 | R$ 204.750,00 |
| 5.4 | BBSSR00289 | Suporte 14x6 - Banco de Horas Mensal - 3hrs - for 36 months | 27022 | 21 | R$ 4.865,00 | R$ 102.165,00 |
| 5.5 | Instalação – 8 horas | Serviço de instalação | 26972 | 21 | R$ 1.632,50 | R$ 34.282,50 |
| **VALOR GLOBAL** | | | | | | **R$ 9.573.789,21** |

**1.2.** O objeto da licitação tem a natureza de serviço comum de solução integrada de Firewall NEXT GENERATION composta de Hardware e Software de segurança da informação do tipo UTM (Unified Threat Management), composta de Hardware e Software de segurança da informação do tipo UTM (Unified Threat Management) entendendo-se como tais o conjunto de serviços e recursos de: Filtro de pacotes com controle de estado, Filtro de conteúdo web, Interceptação SSL, Filtro de aplicações, Controle da web 2.0, Inspeção com proteção contra ataques de Malwares, vírus, worm, e aplicativos maliciosos, integrar soluções do tipo (IPS, ATP, QoS, Balanceamento de serviços, Redundância de links, SD-WAN, VPN, DHCP e DNS), com a capacidade de integrar todos os recursos em um único dispositivo.

1.3.1 Todos os produtos e serviços deverão ser orçados para um período mínimo de vigência do contrato e deverá permitir a atualização do software e do sistema operacional, bem como as atualizações para todas as versões do produto que forem lançadas durante o período do contrato.

**1.3.** Os quantitativos e respectivos códigos dos itens são os discriminados na tabela acima.

**1.4.** A presente contratação adotará como regime de execução empreitada por preço unitário.

**1.5.** O contrato terá vigência pelo período de 36 (meses), podendo ser prorrogado por mais 12 (doze) meses, com base no artigo 57, IV e §1º, da Lei n. 8.666/93.

## 2. JUSTIFICATIVA E OBJETIVO DA CONTRATAÇÃO

A SEDUC-PI adquiriu, em 2017, a principal solução de proteção de rede (Firewall UTM) para as unidades remotas, a qual tem atendido satisfatoriamente às necessidades da organização. A solução de segurança de UTM inclui: filtro de pacote, controle de aplicação, administração de largura de banda (QoS), VPN IPSec e SSL, IPS, prevenção contra ameaças de vírus, spywares, Filtro de URL, bem como controle de transmissão de dados e acesso à internet. Esta solução é do Fabricante BLOCKBIT.

Tendo em vista todo o tempo e investimento realizado para consolidação das tecnologias utilizadas, capacitação da equipe, implantação das soluções e centralização das funcionalidades, entende-se que o ambiente de segurança precisa ser estendido às novas Unidades Operacionais que estão atualmente sem nenhuma proteção e controle. visando manter a uniformidade do ambiente e a integração com a consoles de gerenciamento que possuem licenciamento vigente, fazendo assim que

fique devidamente resguardado o princípio da economicidade pública, haja vista que, caso seja implantado uma solução diferente da já adquirida, será dispensado um investimento de grande vulto, de forma desnecessária, uma vez que já existe base suficiente para continuidade dos equipamentos a serem a adquiridos.

Com o objetivo de além de aumentar a capilaridade da rede garantindo, a segurança da operação e estender o alcance da rede e, ao mesmo tempo, permitir a identificação dos usuários, é necessário que os equipamentos de rede estejam atualizados e em garantia afim de obter pleno funcionamento da rede informática da SEDUC-PI. Com tudo, faz-se necessário que os equipamentos novos tenham interoperabilidade com a atual solução (hardware e software) e se mantenham compatíveis com o mecanismo de segurança adquirido e implementado pelo órgão.

Cumpre ressaltar que a proposição pela aquisição de novas licenças de hardware e software já existentes no parque tecnológico da SEDUC-PI com indicação de marca e modelo do software de solução de segurança de TI traz enorme vantajosidade para a Entidade sendo tecnicamente justificável, pois, de forma complementar aos Regulamentos de Licitações do deste órgão, prevê o parágrafo 5°, artigo 7°, da lei 8.666/93, que caberá a aquisição de material sem similaridade, SALVO nos casos em que for tecnicamente justificável, como é objeto da presente aquisição. Podemos citar também o disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I – Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), todos os itens desse edital, por questões de compatibilidade, gerência, suporte e garantia, devem ser do mesmo fabricante.

Além disso, pode-se citar o entendimento pacificado do TCU, nos termos do acordão nº 849/2012 – transcrito abaixo:

> ACORDAM os Ministros do Tribunal de Contas da União, reunidos em sessão do Plenário, com fundamento nos arts. 85 e 89 do Regimento Interno do TCU e ante as razões expostas pelo Relator, em aprovar o presente projeto de súmula, nos seguintes termos: “Em licitações referentes a compras, inclusive de softwares, é possível a indicação de marca, desde que seja estritamente necessária para atender a exigências de padronização e que haja prévia justificação.”

O Objeto deste termo de referência é considerado material comum, assim entendido como aquele que se apresenta sob identidade e características padronizadas e que se encontra disponível, a qualquer tempo, num mercado próprio. Constitui objeto comparável entre si, visto que pode ser executado mecanicamente ou segundo protocolos, métodos, regulamentos e técnicas pré-estabelecidos e conhecidos por todas as empresas que atuam no ramo.

Temos como objetivo relevante esta nova aquisição a proteção dos dados pessoais dos alunos que trafegam na rede de dados deste órgão. Recentemente tivemos no Brasil a regulamentação das atividades de tratamento de dados pessoais com a Lei nº 13.709/2018, conhecida como a Lei Geral de Proteção de Dados Pessoais (LGPD ou LGPDP). Além das mudanças que tornaram mais rígidas com a alteração dos artigos 7ºe 16º do Marco civil da Internet.

O art. 46 da LGPD traz o seguinte texto:

> “Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.”

A solução principal capaz de executar essa tarefa é justamente o objeto desta licitação, ou seja, o Firewall UTM.

Sendo assim, justifica-se aquisição de firewalls e licenciamento do fabricante BLOCKBIT, pois o papel que o referido equipamento exerce no ambiente de TI da SEDUC-PI é de grande relevância técnica à Entidade, visto que, a ausência dessas soluções representa risco a preservação da segurança da informação e a própria disponibilidade dos serviços prestados pela instituição.

## 3. DESCRIÇÃO DA SOLUÇÃO:

### 3.1. ITEM 1: RENOVAÇÃO BB10

#### 3.1.1. ESPECIFICAÇÕES GERIAS DE SOFTWARE UTM

##### 3.1.1.1. FUNÇÕES BÁSICAS:

- Hardware (Appliances) que atuam na segurança e performance do ambiente de rede;
- VPN SSL, VPN IPSec (Client-to-site e Site-to-site);
- Controle de Aplicações;
- Proxy Web e Filtro de Conteúdo Web (URL Filtering);
- Detecção e prevenção de intrusos – IPS;
- Qualidade de serviço – QOS;
- Anti-Malware;
- SD-WAN;
- Cluster.

##### 3.1.1.2. CARACTERÍSTICAS GERAIS

- A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
- Interface em português e inglês;
- O sistema deve permitir o acesso à interface de gerenciamento WEB por qualquer interface de rede configurada;
- O software deverá ser fornecido em sua versão mais atualizada, não sendo permitido qualquer tipo de comprovação futura.
- Todo o ambiente deverá ser gerenciado sem a necessidade de produtos de terceiros para compor a solução.
- Tanto os Gateways de Segurança bem como a Gerência Centralizada deverão suportar monitoramento através de SNMP v1, v2 e v3.
- A Solução deverá prover inspeção SSL:
- A solução deverá ser em hardware dedicado tipo appliance com sistema operacional customizado para garantir segurança e melhor desempenho.
- Deve ser totalmente gerenciável remotamente, através de rede local, sem a necessidade de instalação de mouse, teclado e monitor de vídeo;
- Deve suportar cluster do tipo Failover (HA) com replicação da tabela de estado.

##### 3.1.1.3. DAS FUNCIONALIDADES DO FIREWALL:

- Possuir capacidade de processamento de pacotes e interfaces de acordo com a tabela de performance dos equipamentos;
- Permitir a conexão simultânea de vários administradores, com poderes de alteração de configurações e/ou apenas de visualização das mesmas;
- Possuir um sistema de armazenamento remoto para salvar backups da solução com suporte a conexões do tipo Network File System, SSH e PenDrive;
- Possibilitar a visualização dos países de origem e destino nos logs de eventos, de acessos e ameaças.
- Possuir mecanismo que permita a realização de cópias de segurança (backups) do sistema e restauração remota, através da interface gráfica, a solução deve permitir o agendamento diário ou semanal;
- O sistema deve permitir configurar o período ou número de cópias que deseja manter no repositório remoto e executar a manutenção de período automaticamente.
- As cópias de segurança devem ser salvas compactadas e criptografadas de forma a garantir segurança, confiabilidade e confidencialidade dos arquivos de backup;

- O sistema ainda deve contemplar um recurso de cópia de segurança do tipo snapshot, que contemple a cópia completa das configurações dos serviços e recursos do sistema;
- Deve possibilitar a restauração do snapshot através da interface web de qualquer ponto remoto, de modo a contribuir para uma restauração imediata sem a necessidade de reinicialização do sistema;
- Deve permitir habilitar ou desabilitar o registro de log por política de firewall.
- Possuir controle de acesso à internet por endereço IP de origem e destino;
- Possuir controle de acesso à internet por sub-rede;
- Possuir suporte a tags de VLAN (802.1q);
- Suportar agregação de links, segundo padrão IEEE 802.3ad;
- Possuir ferramenta de diagnóstico do tipo tcpdump;
- Possuir integração com Servidores de Autenticação RADIUS, TACACS+, LDAP e Microsoft Active Directory;
- Possuir métodos de autenticação de usuários para qualquer aplicação que se execute sob os protocolos TCP ( HTTP, HTTPS, FTP e Telnet);
- Possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation), um para um, N-para-um e vários para um.
- Permitir controle de acesso à internet por períodos do dia, permitindo a aplicação de políticas por horários e por dia da semana;
- Permitir controle de acesso à internet por domínio, exemplo: gov.br, org.br, edu.br;
- Possuir a funcionalidade de fazer tradução de endereços dinâmicos, muitos para um, PAT.
- Possuir suporte a roteamento dinâmico RIP V1, V2, OSPF, BGP;
- Possuir funcionalidades de DHCP Cliente, Servidor e Relay;
- Deverá suportar aplicações multimídia como: H.323, SIP;
- Possuir tecnologia de firewall do tipo Stateful;
- Possuir alta disponibilidade (HA), trabalhando no esquema de redundância do tipo ativo-passivo;
- Permitir o funcionamento em modo transparente tipo “bridge”;
- Permitir a criação de pelo menos 20 VLANS no padrão IEEE 802.1q;
- Possuir conexão entre estação de gerência e appliance criptografada tanto em interface gráfica quanto em CLI (linha de comando);
- Deverá suportar forwarding de multicast;
- Permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos, TCP, UDP, ICMP e IP;
- Permitir o agrupamento de serviços;
- Permitir o filtro de pacotes sem a utilização de NAT;
- Permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas;
- Possuir mecanismo de anti-spoofing;
- Permitir criação de regras definidas pelo usuário;
- Permitir o serviço de autenticação para HTTP e FTP;
- Possuir a funcionalidade de balanceamento e contingência de links;
- Deverá ter técnicas de detecção de programas de compartilhamento de arquivos (peer-to-peer) e de mensagens instantâneas, suportando ao menos: Yahoo! Messenger, MSN Messenger, ICQ, AOL Messenger, BitTorrent, eDonkey, GNUTella, KaZaa, Skype e WinNY.

**3.1.1.4. IDENTIFICAÇÃO DE USUÁRIO:**

- Deve possuir a capacidade de criação de políticas de acesso de Firewall, VPN, IPS e Controle de aplicação integradas ao repositório de usuários sendo: Active Directory, LDAP, TACAC´S e Radius;

- Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- Para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador (Captive Portal), sem a necessidade de agente;
- Deve possuir Captive Portal com suporte a Autenticação Social (Facebook, Twitter, Google);
- A solução deverá ser capaz de identificar nome do usuário, login, máquina/computador registrados no Microsoft Active Directory;
- Na integração com o AD, todos os domain controllers em operação na rede do cliente devem ser cadastrados de maneira simples e sem utilização de scritps de comando;
- A solução de identificação de usuário deverá se integrar com as funcionalidades Firewall, controle de aplicação e IPS, sendo elas do mesmo fabricante;
- A solução deve suportar a opção de instalação de softwares agentes nos PCs/Laptops para que os próprios PCs/Laptops enviem suas credenciais de IP/nome de usuário do domínio/nome da máquina para o gateway diretamente, sem que o Gateway tenha que fazer Queries no AD;

**3.1.1.5. DAS FUNCIONALIDADES DA VPN:**

- VPN baseada em appliance;
- Possuir algoritmos de criptografia para túneis VPN: AES, DES, 3DES;
- Suporte a certificados PKI X.509 para construção de VPNs;
- Possuir suporte a VPNs IPSec site-to-site:
- Criptografia, 3DES, AES128, AES256, AES-GCM-128
- Integridade MD5, SHA-1, SHA-256, SHA384 e AES-XCBC;
- Algoritmo Internet Key Exchange (IKE) versões I e II;
- AES 128 e 256 (Advanced Encryption Standard);
- Suporte a Diffie-Hellman Grupo 1, Grupo 2, Grupo 5, Grupo 14; Grupo 15, Grupo 16, Grupo 17, Grupo 18, Grupo 19, Grupo 20, Grupo 21, Grupo 22, Grupo 23, Grupo 24, Grupo 25, Grupo 26, Grupo 27, Grupo 28, Grupo 29, Grupo 30;
- Possuir suporte a VPN SSL;
- Possuir capacidade de realizar SSL VPNs utilizando certificados digitais;
- A VPN SSL deve possibilitar o acesso a toda infra-estrutura da contratante de acordo com a política de segurança, através de um plug-in ActiveX e/ou Java;
- Deve permitir a arquitetura de vpn hub and spoke;
- Suporte a VPNs IPSec client-to-site;
- Deverá possuir cliente próprio para Windows para o estabelecimento da VPN client-to-site.
- Suporte à inclusão em autoridades certificadoras (enrollment) mediante SCEP (Simple Certificate Enrollment Protocol);
- Possuir funcionalidades de Auto-Dicovery VPN capaz de permitir criar tuneis de VPN dinâmicos entre múltiplos dispositivos (spokes) com um gateway centralizador (hub).;
- A funcionalidade de AD-VPN deve suportar criar os seguintes tipos de tuneis:
- Site-to-Site;
- Full-Mesh;
- Star.

**3.1.1.6. DAS FUNCIONALIDADES DA DETECÇÃO DE INTRUSÃO:**

- A Detecção de Intrusão deverá ser baseada em appliance:
- Capacidade de detecção de mais de 22.000 ataques;
- O Sistema de detecção e proteção de intrusão deverá estar orientado à proteção de redes;

- Possuir tecnologia de detecção baseada em assinatura;
- O sistema de detecção e proteção de intrusão deverá possuir integração à plataforma de segurança;
- Possuir capacidade de remontagem de pacotes para identificação de ataques;
- Deverá possuir capacidade de agrupar assinaturas para um determinado tipo de ataque; Exemplo: agrupar todas as assinaturas relacionadas a web-server para que seja usado para proteção específica de Servidores Web;
- Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep;
- Mecanismos de detecção/proteção de ataques;
- Reconhecimento de padrões;
- Análise de protocolos;
- Detecção de anomalias;
- Detecção de ataques de RPC (Remote procedure call);
- Proteção contra ataques de Windows ou NetBios;
- Proteção contra ataques de SMTP (Simple Message Transfer Protocol) IMAP (Internet Message Access Protocol, Sendmail ou POP (Post Office Protocol);
- Proteção contra ataques DNS (Domain Name System);
- Proteção contra ataques a FTP, SSH , Telnet e rlogin;
- Proteção contra ataques de ICMP (Internet Control Message Protocol);
- Alarmes na console de administração;
- Alertas via correio eletrônico;
- Monitoração do comportamento do appliance através de SNMP, o dispositivo deverá ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede;
- Capacidade de resposta/logs ativa a ataques;
- Terminação de sessões via TCP resets;
- Atualizar automaticamente as assinaturas para o sistema de detecção de intrusos;
- O Sistema de detecção de Intrusos deverá atenuar os efeitos dos ataques de negação de serviços;
- Possuir filtros de ataques por anomalias;
- Permitir filtros de anomalias de tráfego estatístico de: flooding, scan, source e destination session limit;
- Permitir filtros de anomalias de protocolos;
- Suportar reconhecimento de ataques de DoS, reconnaissance, exploits e evasion;
- Suportar verificação de ataque nas camadas de aplicação;

**3.1.1.7. DAS FUNCIONALIDADES DE QOS:**

- Adotar solução de Qualidade de Serviço baseada em appliance;
- Permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound) através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS;
- Permitir modificação de valores DSCP para o DiffServ;
- Limitar individualmente a banda utilizada por programas de compartilhamento de arquivos do tipo peer-to-peer;
- Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;
- Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP;
- Deverá controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP;

- Deverá controlar (limitar ou expandir) individualmente a banda utilizada por sub-rede de origem e destino;
- Deverá controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino;

**3.1.1.8. DAS FUNCIONALIDADES DO ANTIVÍRUS:**

- Possuir funções de Antivírus, Anti-spyware;
- Possuir antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, SMTP, POP3 e FTP;
- Permitir o bloqueio de malwares (adware, spyware, hijackers, keyloggers, etc.)
- Permitir o bloqueio de download de arquivos por extensão e tipo de arquivo;
- Permitir o bloqueio de download de arquivos por tamanho,

**3.1.1.9. DAS FUNCIONALIDADES DO PROXY E FILTRO DE CONTEÚDO WEB:**

- Possuir solução de filtro de conteúdo web integrado a solução de segurança
- Possuir pelo menos 75 categorias para classificação de sites web
- Possuir base mínima contendo, 40 milhões de sites internet web já registrados e classificados;
- Possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites web como:
- Webmail;
- Instituições de Saúde;
- Notícias;
- Pornografia;
- Restaurante;
- Mídias Sociais;
- Esporte;
- Educação;
- Games;
- Compras;
- Permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários;
- Integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados;
- Prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;
- Exibir mensagens de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança da contratante;
- Permitir a filtragem de todo o conteúdo do tráfego WEB de URLs conhecidas como fonte de material impróprio e códigos (programas/scripts) maliciosos em applets Java, cookies, activeX através de: base de URL própria atualizável;
- Permitir o bloqueio de páginas web através da construção de filtros específicos com mecanismo de busca textual;
- Permitir a criação de listas personalizadas de URLs permitidas – lista branca e bloqueadas – lista negra;
- Deverá permitir o bloqueio de URLs inválidas cujo campo CN do certificado SSL não contém um domínio válido;
- Garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo web;
- Deverá permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP;
- Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;

- Deverá permitir a criação de regras para acesso/bloqueio por sub-rede de origem;
- Deverá ser capaz de categorizar a página web tanto pela sua URL como pelo seu endereço IP;
- Deverá permitir o bloqueio de páginas web por Classificação como páginas que facilitam a busca de Audio, Video e URLs originadas de Spam;
- Deverá permitir a criação de listas personalizadas de URLs permitidas – lista branca e bloqueadas – lista negra;
- Deverá funcionar em modo Proxy Explícito para HTTP, HTTPS, e FTP e em Proxy Transparente;
- Deverá permitir configurar a porta do Proxy Explícito.

**3.1.1.10. DAS FUNCIONALIDADES DO CONTROLE DE APLICAÇÕES:**

- As funcionalidades abaixo devem ser baseadas em appliance:
- Deverá reconhecer no mínimo 700 aplicações;
- Deverá possuir pelo menos 10 categorias para classificação de aplicações;
- Deverá possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações como:
- P2P;
- Web;
- Transferência de arquivos;
- Chat;
- Social;
- Deverá permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários;
- Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;
- Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;
- Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory;
- Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP;
- Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;
- Deverá permitir a criação de regras para acesso/bloqueio por sub-rede de origem e destino;
- Deverá garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações.

**3.1.1.11. SISTEMA DE PROTEÇÃO AVANÇADA CONTRA AMEAÇAS – ATP:**

- Possuir sistema de proteção avançada contra ameaças (ATP) nativo;
- O sistema de ATP deve monitorar e analisar o tráfego da rede, identificar aplicativos e ameaças de ataques direcionados e persistentes e efetuar os respectivos bloqueios.
- Deve ser baseado em uma lista de assinaturas eletrônicas que atue em tempo real analisando a camada de aplicação, capaz de identificar o conteúdo dos pacotes, fazer log (registros) das assinaturas trafegadas, inspecionar os pacotes e efetuar o descarte automático do pacote quando identificado assinaturas de pacotes maliciosos, inapropriados para o uso no ambiente corporativo;
- A base de assinaturas do sistema de ATP nativo deverá ser fornecida pelo período do contrato;
- Possuir um mínimo de 31 mil (trinta e um mil) assinaturas;

- Dever permitir a identificação de aplicativos e ameaças independente das portas e protocolos;
- Deve permitir a atualização automática das assinaturas por meio de agendamento diário;
- Possuir capacidade de inspecionar e bloquear em tempo real, ameaças do tipo: activex, malware, malware-backdoors, ataques P2P, trojans, worms, user_agents, pua (adware, p2p, toolbars) malwares para mobile, blacklist, botcc, exploits-kits, file-executable, file-flash, file-identify, file-image, file-java, file-multimedia, file-office, file-other, file-pdf, games, inappropriate e vulnerabilidades conhecidas;
- Possuir uma ferramenta de bloqueio de execução de aplicativos, integrado a base de Antivírus e Antimalware;
- Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos do tipo: ads, cloud, colaboração, download, e-mail, games, mobile, p2p, proxy, remote, redes sociais; storage, streaming, update, voip e web.
- Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos de VoIP tais como: Hotline, Asterisk, Linphone, SIP, Skype, Xlite SIP, X-Pro SIP, Cisco SIP, OpenSIP, Bria, ClearSea e Nero SIP;
- Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos de Redes Sociais tais como: Aol Instant Messenger, Badoo, BaiduHi, Airtime, Blogger, BoldChat, ChatON, China.com, Facebook, Flickr, FC2, Fring, Google Analytics, Google App, ICQ, Linkdin, Meetup, MSM Messenger, Netlog, Skype, Tinder, Tuenti, Twitter, WhatssApp, WeChat e Zoho Chat;
- Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos e transferências de arquivos do tipo P2P (peer to peer) tais como: BitTorrent, Gnutella, FastTrack, IceShare, Napster, Shareman e de Storages, tais como: Dropbox, Easy-share, Google Drive, Megashare, MegaUpload, Rapidshare, OneDrive, Yahoo Box, SoundCloud e Filemail, DivShare;
- Suportar exceção de ameaças por assinatura; IP de origem ou IP de destino;
- Suportar exceção de aplicativos por assinatura; IP de origem ou IP de destino;
- Deve possuir mecanismos para gerar gráfico do histórico da relação de eventos entre as “ameaças detectadas” e as “ameaças bloqueadas”;
- Deve possuir mecanismos para gerar gráfico do histórico da relação de eventos entre os “aplicativos detectados” e os “aplicativos bloqueados”;
- Deve possuir mecanismos para gerar log dos registros das incidências, classificados em pelo menos 3 (três) níveis de impacto: “baixo; médio e alto”;
- Gerar registro do tipo Top Level, dos 10(dez) mais, inclusive da relação de eventos entre usuários e ameaças, usuário e aplicativos, aplicativos e ameaças identificados e bloqueados;

**3.1.1.12. WAN DEFINIDA POR SOFTWARE - SD-WAN:**

- Possuir funcionalidades de SD-WAN, não se limitando aos recursos solicitados abaixo;
- Possuir o balanceamento automático para conexões externas à internet através das interfaces físicas;
- Permitir utilizar VPN IPsec para interligar unidades remotas;
- Possuir recurso de “persistência de link” para impedir a queda de conexões em aplicações que não suportam o load balance de link;
- O balanceamento deverá ser baseado em critérios de desempenho, devendo no mínimo, permitir verificar o monitoramento do consumo de banda, perda de pacotes, jitter e latência;
- Deve possuir uma janela web ou dashboard capaz de fornecer informações dos eventos relacionado ao recurso SD-WAN;
- Deverá oferecer um monitor capaz de prover em tempo real as seguintes informações:

- Consumo de banda;
- Perda de pacotes;
- Jitter;
- Latência.

#### 3.1.1.13. ALTA DISPONIBILIDADE

- Possuir mecanismo de Alta Disponibilidade operando em modo Ativo/Standby, com as implementações de Fail Over.
- Não serão permitidas soluções de cluster (HA) que façam com que o equipamento (s) reinicie após qualquer modificação de parâmetro/configuração seja realizada pelo administrador.
- O Sincronismo dos servidores deve ser por interface exclusiva permitindo utilizar mais de uma interface de Heartbeat;

### 3.1.2. SERVIÇOS DE SUPORTE TÉCNICO REMOTO 14X6 – RENOVAÇÃO BB 10:

- Serviço de suporte REMOTO para os equipamentos de segurança de borda contratados, no horário 14X6(Segunda a sábado das 08:00 às 22:00, exceto feriados), pelo tempo de contrato, com as seguintes características:
- A contratada deve possuir serviço de abertura de chamados remoto capaz de abrir chamados de forma centralizada, em caso de ocorrências de defeitos e/ou falhas na rede relativos aos equipamentos e/ou produtos fornecidos;
- A contratada deverá iniciar o atendimento de suporte em no máximo 8 horas úteis após a abertura do chamado;
- A contratada deverá fornecer atestado comprovando a existência de equipe técnica de no mínimo 3 pessoas capacitadas em todas as soluções adquiridas. O atestado deverá ser fornecido pelo fabricante;
- A CONTRATADA será eximida da aplicação das sanções administrativas para os respectivos chamados em que sejam descumpridos os tempos de solução, desde que comprovadas as seguintes situações: Quando constatado que o problema está relacionado a “bug” no produto e que o fabricante não possui uma correção imediata para tal, sendo este fato declarado pelo próprio;
- A CONTRATADA tomou todas as medidas possíveis visando providenciar solução de contorno;

## 3.2. ITEM 2: RENOVAÇÃO BB 10000

### 3.2.1. ESPECIFICAÇÕES GERIAS DE SOFTWARE UTM

#### 3.2.1.1. FUNÇÕES BÁSICAS:

- Hardware (Appliances) que atuam na segurança e performance do ambiente de rede;
- VPN SSL, VPN IPSec (Client-to-site e Site-to-site);
- Controle de Aplicações;
- Proxy Web e Filtro de Conteúdo Web (URL Filtering);
- Detecção e prevenção de intrusos – IPS;
- Qualidade de serviço – QOS;
- Anti-Malware;
- SD-WAN;
- Cluster.

#### 3.2.1.2. CARACTERÍSTICAS GERAIS:

- A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
- Interface em português e inglês;

- O sistema deve permitir o acesso à interface de gerenciamento WEB por qualquer interface de rede configurada;
- O software deverá ser fornecido em sua versão mais atualizada, não sendo permitido qualquer tipo de comprovação futura.
- Todo o ambiente deverá ser gerenciado sem a necessidade de produtos de terceiros para compor a solução.
- Tanto os Gateways de Segurança bem como a Gerência Centralizada deverão suportar monitoramento através de SNMP v1, v2 e v3.
- A Solução deverá prover inspeção SSL:
- A solução deverá ser em hardware dedicado tipo appliance com sistema operacional customizado para garantir segurança e melhor desempenho.
- Deve ser totalmente gerenciável remotamente, através de rede local, sem a necessidade de instalação de mouse, teclado e monitor de vídeo;
- Deve suportar cluster do tipo Failover (HA) com replicação da tabela de estado.

**3.2.1.3. DAS FUNCIONALIDADES DO FIREWALL:**

- Possuir capacidade de processamento de pacotes e interfaces de acordo com a tabela de performance dos equipamentos;
- Permitir a conexão simultânea de vários administradores, com poderes de alteração de configurações e/ou apenas de visualização das mesmas;
- Possuir um sistema de armazenamento remoto para salvar backups da solução com suporte a conexões do tipo Network File System, SSH e PenDrive;
- Possibilitar a visualização dos países de origem e destino nos logs de eventos, de acessos e ameaças.
- Possuir mecanismo que permita a realização de cópias de segurança (backups) do sistema e restauração remota, através da interface gráfica, a solução deve permitir o agendamento diário ou semanal;
- O sistema deve permitir configurar o período ou número de cópias que deseja manter no repositório remoto e executar a manutenção de período automaticamente.
- As cópias de segurança devem ser salvas compactadas e criptografadas de forma a garantir segurança, confiabilidade e confidencialidade dos arquivos de backup;
- O sistema ainda deve contemplar um recurso de cópia de segurança do tipo snapshot, que contemple a cópia completa das configurações dos serviços e recursos do sistema;
- Deve possibilitar a restauração do snapshot através da interface web de qualquer ponto remoto, de modo a contribuir para uma restauração imediata sem a necessidade de reinicialização do sistema;
- Deve permitir habilitar ou desabilitar o registro de log por política de firewall.
- Possuir controle de acesso à internet por endereço IP de origem e destino;
- Possuir controle de acesso à internet por sub-rede;
- Possuir suporte a tags de VLAN (802.1q);
- Suportar agregação de links, segundo padrão IEEE 802.3ad;
- Possuir ferramenta de diagnóstico do tipo tcpdump;
- Possuir integração com Servidores de Autenticação RADIUS, TACACS+, LDAP e Microsoft Active Directory;
- Possuir métodos de autenticação de usuários para qualquer aplicação que se execute sob os protocolos TCP ( HTTP, HTTPS, FTP e Telnet);
- Possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation), um para um, N-para-um e vários para um.
- Permitir controle de acesso à internet por períodos do dia, permitindo a aplicação de políticas por horários e por dia da semana;
- Permitir controle de acesso à internet por domínio, exemplo: gov.br, org.br, edu.br;

- Possuir a funcionalidade de fazer tradução de endereços dinâmicos, muitos para um, PAT.
- Possuir suporte a roteamento dinâmico RIP V1, V2, OSPF, BGP;
- Possuir funcionalidades de DHCP Cliente, Servidor e Relay;
- Deverá suportar aplicações multimídia como: H.323, SIP;
- Possuir tecnologia de firewall do tipo Stateful;
- Possuir alta disponibilidade (HA), trabalhando no esquema de redundância do tipo ativo-passivo;
- Permitir o funcionamento em modo transparente tipo “bridge”;
- Permitir a criação de pelo menos 20 VLANS no padrão IEEE 802.1q;
- Possuir conexão entre estação de gerência e appliance criptografada tanto em interface gráfica quanto em CLI (linha de comando);
- Deverá suportar forwarding de multicast;
- Permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos, TCP, UDP, ICMP e IP;
- Permitir o agrupamento de serviços;
- Permitir o filtro de pacotes sem a utilização de NAT;
- Permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas;
- Possuir mecanismo de anti-spoofing;
- Permitir criação de regras definidas pelo usuário;
- Permitir o serviço de autenticação para HTTP e FTP;
- Possuir a funcionalidade de balanceamento e contingência de links;
- Deverá ter técnicas de detecção de programas de compartilhamento de arquivos (peer-to-peer) e de mensagens instantâneas, suportando ao menos: Yahoo! Messenger, MSN Messenger, ICQ, AOL Messenger, BitTorrent, eDonkey, GNUTella, KaZaa, Skype e WinNY.

**3.2.1.4. IDENTIFICAÇÃO DE USUÁRIO:**

- Deve possuir a capacidade de criação de políticas de acesso de Firewall, VPN, IPS e Controle de aplicação integradas ao repositório de usuários sendo: Active Directory, LDAP, TACAC´S e Radius;
- Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- Para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador (Captive Portal), sem a necessidade de agente;
- Deve possuir Captive Portal com suporte a Autenticação Social (Facebook, Twitter, Google);
- A solução deverá ser capaz de identificar nome do usuário, login, máquina/computador registrados no Microsoft Active Directory;
- Na integração com o AD, todos os domain controllers em operação na rede do cliente devem ser cadastrados de maneira simples e sem utilização de scritps de comando;
- A solução de identificação de usuário deverá se integrar com as funcionalidades Firewall, controle de aplicação e IPS, sendo elas do mesmo fabricante;
- A solução deve suportar a opção de instalação de softwares agentes nos PCs/Laptops para que os próprios PCs/Laptops enviem suas credenciais de IP/nome de usuário do domínio/nome da máquina para o gateway diretamente, sem que o Gateway tenha que fazer Queries no AD;

**3.2.1.5. DAS FUNCIONALIDADES DA VPN:**

- VPN baseada em appliance;
- Possuir algoritmos de criptografia para túneis VPN: AES, DES, 3DES;

- Suporte a certificados PKI X.509 para construção de VPNs;
- Possuir suporte a VPNs IPSec site-to-site:
- Criptografia, 3DES, AES128, AES256, AES-GCM-128
- Integridade MD5, SHA-1, SHA-256, SHA384 e AES-XCBC;
- Algoritmo Internet Key Exchange (IKE) versões I e II;
- AES 128 e 256 (Advanced Encryption Standard);
- Suporte a Diffie-Hellman Grupo 1, Grupo 2, Grupo 5, Grupo 14; Grupo 15, Grupo 16, Grupo 17, Grupo 18, Grupo 19, Grupo 20, Grupo 21, Grupo 22, Grupo 23, Grupo 24, Grupo 25, Grupo 26, Grupo 27, Grupo 28, Grupo 29, Grupo 30;
- Possuir suporte a VPN SSL;
- Possuir capacidade de realizar SSL VPNs utilizando certificados digitais;
- A VPN SSL deve possibilitar o acesso a toda infra-estrutura da contratante de acordo com a política de segurança, através de um plug-in ActiveX e/ou Java;
- Deve permitir a arquitetura de vpn hub and spoke;
- Suporte a VPNs IPSec client-to-site;
- Deverá possuir cliente próprio para Windows para o estabelecimento da VPN client-to-site.
- Suporte à inclusão em autoridades certificadoras (enrollment) mediante SCEP (Simple Certificate Enrollment Protocol);
- Possuir funcionalidades de Auto-Dicovery VPN capaz de permitir criar tuneis de VPN dinâmicos entre múltiplos dispositivos (spokes) com um gateway centralizador (hub).;
- A funcionalidade de AD-VPN deve suportar criar os seguintes tipos de tuneis:
- Site-to-Site;
- Full-Mesh;
- Star.

**3.2.1.6. DAS FUNCIONALIDADES DA DETECÇÃO DE INTRUSÃO:**

- A Detecção de Intrusão deverá ser baseada em appliance:
- Capacidade de detecção de mais de 22.000 ataques;
- O Sistema de detecção e proteção de intrusão deverá estar orientado à proteção de redes;
- Possuir tecnologia de detecção baseada em assinatura;
- O sistema de detecção e proteção de intrusão deverá possuir integração à plataforma de segurança;
- Possuir capacidade de remontagem de pacotes para identificação de ataques;
- Deverá possuir capacidade de agrupar assinaturas para um determinado tipo de ataque; Exemplo: agrupar todas as assinaturas relacionadas a web-server para que seja usado para proteção específica de Servidores Web;
- Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep;
- Mecanismos de detecção/proteção de ataques;
- Reconhecimento de padrões;
- Análise de protocolos;
- Detecção de anomalias;
- Detecção de ataques de RPC (Remote procedure call);
- Proteção contra ataques de Windows ou NetBios;
- Proteção contra ataques de SMTP (Simple Message Transfer Protocol) IMAP (Internet Message Access Protocol, Sendmail ou POP (Post Office Protocol);
- Proteção contra ataques DNS (Domain Name System);
- Proteção contra ataques a FTP, SSH , Telnet e rlogin;
- Proteção contra ataques de ICMP (Internet Control Message Protocol);
- Alarmes na console de administração;
- Alertas via correio eletrônico;

- Monitoração do comportamento do appliance através de SNMP, o dispositivo deverá ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede;
- Capacidade de resposta/logs ativa a ataques;
- Terminação de sessões via TCP resets;
- Atualizar automaticamente as assinaturas para o sistema de detecção de intrusos;
- O Sistema de detecção de Intrusos deverá atenuar os efeitos dos ataques de negação de serviços;
- Possuir filtros de ataques por anomalias;
- Permitir filtros de anomalias de tráfego estatístico de: flooding, scan, source e destination session limit;
- Permitir filtros de anomalias de protocolos;
- Suportar reconhecimento de ataques de DoS, reconnaissance, exploits e evasion;
- Suportar verificação de ataque nas camadas de aplicação;

**3.2.1.7. DAS FUNCIONALIDADES DE QOS:**

- Adotar solução de Qualidade de Serviço baseada em appliance;
- Permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound) através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS;
- Permitir modificação de valores DSCP para o DiffServ;
- Limitar individualmente a banda utilizada por programas de compartilhamento de arquivos do tipo peer-to-peer;
- Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;
- Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP;
- Deverá controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP;
- Deverá controlar (limitar ou expandir) individualmente a banda utilizada por sub-rede de origem e destino;
- Deverá controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino;

**3.2.1.8. DAS FUNCIONALIDADES DO ANTIVÍRUS:**

- Possuir funções de Antivírus, Anti-spyware;
- Possuir antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, SMTP, POP3 e FTP;
- Permitir o bloqueio de malwares (adware, spyware, hijackers, keyloggers, etc.)
- Permitir o bloqueio de download de arquivos por extensão e tipo de arquivo;
- Permitir o bloqueio de download de arquivos por tamanho.

**3.2.1.9. DAS FUNCIONALIDADES DO PROXY E FILTRO DE CONTEÚDO WEB:**

- Possuir solução de filtro de conteúdo web integrado a solução de segurança
- Possuir pelo menos 75 categorias para classificação de sites web
- Possuir base mínima contendo, 40 milhões de sites internet web já registrados e classificados;
- Possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites web como:
- Webmail;
- Instituições de Saúde;
- Notícias;

- Pornografia;
- Restaurante;
- Mídias Sociais;
- Esporte;
- Educação;
- Games;
- Compras;
- Permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários;
- Integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados;
- Prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;
- Exibir mensagens de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança da contratante;
- Permitir a filtragem de todo o conteúdo do tráfego WEB de URLs conhecidas como fonte de material impróprio e códigos (programas/scripts) maliciosos em applets Java, cookies, activeX através de: base de URL própria atualizável;
- Permitir o bloqueio de páginas web através da construção de filtros específicos com mecanismo de busca textual;
- Permitir a criação de listas personalizadas de URLs permitidas – lista branca e bloqueadas – lista negra;
- Deverá permitir o bloqueio de URLs inválidas cujo campo CN do certificado SSL não contém um domínio válido;
- Garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo web;
- Deverá permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP;
- Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;
- Deverá permitir a criação de regras para acesso/bloqueio por sub-rede de origem;
- Deverá ser capaz de categorizar a página web tanto pela sua URL como pelo seu endereço IP;
- Deverá permitir o bloqueio de páginas web por Classificação como páginas que facilitam a busca de Audio, Video e URLs originadas de Spam;
- Deverá permitir a criação de listas personalizadas de URLs permitidas – lista branca e bloqueadas – lista negra;
- Deverá funcionar em modo Proxy Explícito para HTTP, HTTPS, e FTP e em Proxy Transparente;
- Deverá permitir configurar a porta do Proxy Explícito.

**3.2.1.10. DAS FUNCIONALIDADES DO CONTROLE DE APLICAÇÕES:**

- As funcionalidades abaixo devem ser baseadas em appliance:
- Deverá reconhecer no mínimo 700 aplicações;
- Deverá possuir pelo menos 10 categorias para classificação de aplicações;
- Deverá possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações como:
- P2P;
- Web;
- Transferência de arquivos;
- Chat;
- Social;

- Deverá permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários;
- Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;
- Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;
- Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory;
- Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP;
- Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;
- Deverá permitir a criação de regras para acesso/bloqueio por sub-rede de origem e destino;
- Deverá garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações.

**3.2.1.11. SISTEMA DE PROTEÇÃO AVANÇADA CONTRA AMEAÇAS – ATP:**

- Possuir sistema de proteção avançada contra ameaças (ATP) nativo;
- O sistema de ATP deve monitorar e analisar o tráfego da rede, identificar aplicativos e ameaças de ataques direcionados e persistentes e efetuar os respectivos bloqueios.
- Deve ser baseado em uma lista de assinaturas eletrônicas que atue em tempo real analisando a camada de aplicação, capaz de identificar o conteúdo dos pacotes, fazer log (registros) das assinaturas trafegadas, inspecionar os pacotes e efetuar o descarte automático do pacote quando identificado assinaturas de pacotes maliciosos, inapropriados para o uso no ambiente corporativo;
- A base de assinaturas do sistema de ATP nativo deverá ser fornecida pelo período do contrato;
- Possuir um mínimo de 31 mil (trinta e um mil) assinaturas;
- Dever permitir a identificação de aplicativos e ameaças independente das portas e protocolos;
- Deve permitir a atualização automática das assinaturas por meio de agendamento diário;
- Possuir capacidade de inspecionar e bloquear em tempo real, ameaças do tipo: activex, malware, malware-backdoors, ataques P2P, trojans, worms, user_agents, pua (adware, p2p, toolbars) malwares para mobile, blacklist, botcc, exploits-kits, file-executable, file-flash, file-identify, file-image, file-java, file-multimedia, file-office, file-other, file-pdf, games, inappropriate e vulnerabilidades conhecidas;
- Possuir uma ferramenta de bloqueio de execução de aplicativos, integrado a base de Antivírus e Antimalware;
- Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos do tipo: ads, cloud, colaboração, download, e-mail, games, mobile, p2p, proxy, remote, redes sociais; storage, streaming, update, voip e web.
- Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos de VoIP tais como: Hotline, Asterisk, Linphone, SIP, Skype, Xlite SIP, X-Pro SIP, Cisco SIP, OpenSIP, Bria, ClearSea e Nero SIP;
- Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos de Redes Sociais tais como: Aol Instant Messenger, Badoo, BaiduHi, Airtime, Blogger, BoldChat, ChatON, China.com, Facebook, Flickr, FC2, Fring, Google Analytics, Google App, ICQ, Linkdin, Meetup, MSM Messenger, Netlog, Skype, Tinder, Tuenti, Twitter, WhatssApp, WeChat e Zoho Chat;
- Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos e transferências de arquivos do tipo P2P (peer to peer) tais como: BitTorrent, Gnutella, FastTrack, IceShare, Napster, Shareman e de Storages, tais como: Dropbox, Easy-share, Google Drive,

Megashare, MegaUpload, Rapidshare, OneDrive, Yahoo Box, SoundCloud e Filemail, DivShare;

- Suportar exceção de ameaças por assinatura; IP de origem ou IP de destino;
- Suportar exceção de aplicativos por assinatura; IP de origem ou IP de destino;
- Deve possuir mecanismos para gerar gráfico do histórico da relação de eventos entre as “ameaças detectadas” e as “ameaças bloqueadas”;
- Deve possuir mecanismos para gerar gráfico do histórico da relação de eventos entre os “aplicativos detectados” e os “aplicativos bloqueados”;
- Deve possuir mecanismos para gerar log dos registros das incidências, classificados em pelo menos 3 (três) níveis de impacto: “baixo; médio e alto”;
- Gerar registro do tipo Top Level, dos 10(dez) mais, inclusive da relação de eventos entre usuários e ameaças, usuário e aplicativos, aplicativos e ameaças identificados e bloqueados;

**3.2.1.12. WAN DEFINIDA POR SOFTWARE - SD-WAN:**

- Possuir funcionalidades de SD-WAN, não se limitando aos recursos solicitados abaixo;
- Possuir o balanceamento automático para conexões externas à internet através das interfaces físicas;
- Permitir utilizar VPN IPsec para interligar unidades remotas;
- Possuir recurso de “persistência de link” para impedir a queda de conexões em aplicações que não suportam o load balance de link;
- O balanceamento deverá ser baseado em critérios de desempenho, devendo no mínimo, permitir verificar o monitoramento do consumo de banda, perda de pacotes, jitter e latência;
- Deve possuir uma janela web ou dashboard capaz de fornecer informações dos eventos relacionado ao recurso SD-WAN;
- Deverá oferecer um monitor capaz de prover em tempo real as seguintes informações:
- Consumo de banda;
- Perda de pacotes;
- Jitter;
- Latência.

**3.2.1.13. ALTA DISPONIBILIDADE:**

- Possuir mecanismo de Alta Disponibilidade operando em modo Ativo/Standby, com as implementações de Fail Over.
- Não serão permitidas soluções de cluster (HA) que façam com que o equipamento (s) reinicie após qualquer modificação de parâmetro/configuração seja realizada pelo administrador.
- O Sincronismo dos servidores deve ser por interface exclusiva permitindo utilizar mais de uma interface de Heartbeat;

**3.2.2. SERVIÇOS DE SUPORTE TÉCNICO REMOTO 14X6 – RENOVAÇÃO BB 1000:**

- Serviço de suporte REMOTO para os equipamentos de segurança de borda contratados, no horário 14X6(Segunda a sábado das 08:00 às 22:00, exceto feriados), pelo tempo de contrato, com as seguintes características:
- A contratada deve possuir serviço de abertura de chamados remoto capaz de abrir chamados de forma centralizada, em caso de ocorrências de defeitos e/ou falhas na rede relativos aos equipamentos e/ou produtos fornecidos;
- A contratada deverá iniciar o atendimento de suporte em no máximo 8 horas úteis após a abertura do chamado;

- A contratada deverá fornecer atestado comprovando a existência de equipe técnica de no mínimo 3 pessoas capacitadas em todas as soluções adquiridas. O atestado deverá ser fornecido pelo fabricante;
- A CONTRATADA será eximida da aplicação das sanções administrativas para os respectivos chamados em que sejam descumpridos os tempos de solução, desde que comprovadas as seguintes situações: Quando constatado que o problema está relacionado a “bug” no produto e que o fabricante não possui uma correção imediata para tal, sendo este fato declarado pelo próprio;
- A CONTRATADA tomou todas as medidas possíveis visando providenciar solução de contorno.

## 3.3. ITEM 3: AQUISIÇÃO BB10:

### 3.3.1. ESPECIFICAÇÕES GERIAS DE SOFTWARE UTM

#### 3.3.1.1. FUNÇÕES BÁSICAS:

- Hardware (Appliances) que atuam na segurança e performance do ambiente de rede;
- VPN SSL, VPN IPSec (Client-to-site e Site-to-site);
- Controle de Aplicações;
- Proxy Web e Filtro de Conteúdo Web (URL Filtering);
- Detecção e prevenção de intrusos – IPS;
- Qualidade de serviço – QOS;
- Anti-Malware;
- SD-WAN;
- Cluster.

#### 3.3.1.2. CARACTERÍSTICAS GERAIS:

- A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
- Interface em português e inglês;
- O sistema deve permitir o acesso à interface de gerenciamento WEB por qualquer interface de rede configurada;
- O software deverá ser fornecido em sua versão mais atualizada, não sendo permitido qualquer tipo de comprovação futura.
- Todo o ambiente deverá ser gerenciado sem a necessidade de produtos de terceiros para compor a solução.
- Tanto os Gateways de Segurança bem como a Gerência Centralizada deverão suportar monitoramento através de SNMP v1, v2 e v3.
- A Solução deverá prover inspeção SSL:
- A solução deverá ser em hardware dedicado tipo appliance com sistema operacional customizado para garantir segurança e melhor desempenho.
- Deve ser totalmente gerenciável remotamente, através de rede local, sem a necessidade de instalação de mouse, teclado e monitor de vídeo;
- Deve suportar cluster do tipo Failover (HA) com replicação da tabela de estado.

#### 3.3.1.3. DAS FUNCIONALIDADES DO FIREWALL:

- Possuir capacidade de processamento de pacotes e interfaces de acordo com a tabela de performance dos equipamentos;
- Permitir a conexão simultânea de vários administradores, com poderes de alteração de configurações e/ou apenas de visualização das mesmas;
- Possuir um sistema de armazenamento remoto para salvar backups da solução com suporte a conexões do tipo Network File System, SSH e PenDrive;

- Possibilitar a visualização dos países de origem e destino nos logs de eventos, de acessos e ameaças.
- Possuir mecanismo que permita a realização de cópias de segurança (backups) do sistema e restauração remota, através da interface gráfica, a solução deve permitir o agendamento diário ou semanal;
- O sistema deve permitir configurar o período ou número de cópias que deseja manter no repositório remoto e executar a manutenção de período automaticamente.
- As cópias de segurança devem ser salvas compactadas e criptografadas de forma a garantir segurança, confiabilidade e confidencialidade dos arquivos de backup;
- O sistema ainda deve contemplar um recurso de cópia de segurança do tipo snapshot, que contemple a cópia completa das configurações dos serviços e recursos do sistema;
- Deve possibilitar a restauração do snapshot através da interface web de qualquer ponto remoto, de modo a contribuir para uma restauração imediata sem a necessidade de reinicialização do sistema;
- Deve permitir habilitar ou desabilitar o registro de log por política de firewall.
- Possuir controle de acesso à internet por endereço IP de origem e destino;
- Possuir controle de acesso à internet por sub-rede;
- Possuir suporte a tags de VLAN (802.1q);
- Suportar agregação de links, segundo padrão IEEE 802.3ad;
- Possuir ferramenta de diagnóstico do tipo tcpdump;
- Possuir integração com Servidores de Autenticação RADIUS, TACACS+, LDAP e Microsoft Active Directory;
- Possuir métodos de autenticação de usuários para qualquer aplicação que se execute sob os protocolos TCP ( HTTP, HTTPS, FTP e Telnet);
- Possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation), um para um, N-para-um e vários para um.
- Permitir controle de acesso à internet por períodos do dia, permitindo a aplicação de políticas por horários e por dia da semana;
- Permitir controle de acesso à internet por domínio, exemplo: gov.br, org.br, edu.br;
- Possuir a funcionalidade de fazer tradução de endereços dinâmicos, muitos para um, PAT.
- Possuir suporte a roteamento dinâmico RIP V1, V2, OSPF, BGP;
- Possuir funcionalidades de DHCP Cliente, Servidor e Relay;
- Deverá suportar aplicações multimídia como: H.323, SIP;
- Possuir tecnologia de firewall do tipo Stateful;
- Possuir alta disponibilidade (HA), trabalhando no esquema de redundância do tipo ativo-passivo;
- Permitir o funcionamento em modo transparente tipo “bridge”;
- Permitir a criação de pelo menos 20 VLANS no padrão IEEE 802.1q;
- Possuir conexão entre estação de gerência e appliance criptografada tanto em interface gráfica quanto em CLI (linha de comando);
- Deverá suportar forwarding de multicast;
- Permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos, TCP, UDP, ICMP e IP;
- Permitir o agrupamento de serviços;
- Permitir o filtro de pacotes sem a utilização de NAT;
- Permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas;
- Possuir mecanismo de anti-spoofing;
- Permitir criação de regras definidas pelo usuário;
- Permitir o serviço de autenticação para HTTP e FTP;
- Possuir a funcionalidade de balanceamento e contingência de links;

- Deverá ter técnicas de detecção de programas de compartilhamento de arquivos (peer-to-peer) e de mensagens instantâneas, suportando ao menos: Yahoo! Messenger, MSN Messenger, ICQ, AOL Messenger, BitTorrent, eDonkey, GNUTella, KaZaa, Skype e WinNY.

**3.3.1.4. IDENTIFICAÇÃO DE USUÁRIO:**

- Deve possuir a capacidade de criação de políticas de acesso de Firewall, VPN, IPS e Controle de aplicação integradas ao repositório de usuários sendo: Active Directory, LDAP, TACAC´S e Radius;
- Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- Para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador (Captive Portal), sem a necessidade de agente;
- Deve possuir Captive Portal com suporte a Autenticação Social (Facebook, Twitter, Google);
- A solução deverá ser capaz de identificar nome do usuário, login, máquina/computador registrados no Microsoft Active Directory;
- Na integração com o AD, todos os domain controllers em operação na rede do cliente devem ser cadastrados de maneira simples e sem utilização de scritps de comando;
- A solução de identificação de usuário deverá se integrar com as funcionalidades Firewall, controle de aplicação e IPS, sendo elas do mesmo fabricante;
- A solução deve suportar a opção de instalação de softwares agentes nos PCs/Laptops para que os próprios PCs/Laptops enviem suas credenciais de IP/nome de usuário do domínio/nome da máquina para o gateway diretamente, sem que o Gateway tenha que fazer Queries no AD;

**3.3.1.5. DAS FUNCIONALIDADES DA VPN:**

- VPN baseada em appliance;
- Possuir algoritmos de criptografia para túneis VPN: AES, DES, 3DES;
- Suporte a certificados PKI X.509 para construção de VPNs;
- Possuir suporte a VPNs IPSec site-to-site:
- Criptografia, 3DES, AES128, AES256, AES-GCM-128
- Integridade MD5, SHA-1, SHA-256, SHA384 e AES-XCBC;
- Algoritmo Internet Key Exchange (IKE) versões I e II;
- AES 128 e 256 (Advanced Encryption Standard);
- Suporte a Diffie-Hellman Grupo 1, Grupo 2, Grupo 5, Grupo 14; Grupo 15, Grupo 16, Grupo 17, Grupo 18, Grupo 19, Grupo 20, Grupo 21, Grupo 22, Grupo 23, Grupo 24, Grupo 25, Grupo 26, Grupo 27, Grupo 28, Grupo 29, Grupo 30;
- Possuir suporte a VPN SSL;
- Possuir capacidade de realizar SSL VPNs utilizando certificados digitais;
- A VPN SSL deve possibilitar o acesso a toda infra-estrutura da contratante de acordo com a política de segurança, através de um plug-in ActiveX e/ou Java;
- Deve permitir a arquitetura de vpn hub and spoke;
- Suporte a VPNs IPSec client-to-site;
- Deverá possuir cliente próprio para Windows para o estabelecimento da VPN client-to-site.
- Suporte à inclusão em autoridades certificadoras (enrollment) mediante SCEP (Simple Certificate Enrollment Protocol);
- Possuir funcionalidades de Auto-Dicovery VPN capaz de permitir criar tuneis de VPN dinâmicos entre múltiplos dispositivos (spokes) com um gateway centralizador (hub).;
- A funcionalidade de AD-VPN deve suportar criar os seguintes tipos de tuneis:
- Site-to-Site;

- Full-Mesh;
- Star.

**3.3.1.6. DAS FUNCIONALIDADES DA DETECÇÃO DE INTRUSÃO:**

- A Detecção de Intrusão deverá ser baseada em appliance:
- Capacidade de detecção de mais de 22.000 ataques;
- O Sistema de detecção e proteção de intrusão deverá estar orientado à proteção de redes;
- Possuir tecnologia de detecção baseada em assinatura;
- O sistema de detecção e proteção de intrusão deverá possuir integração à plataforma de segurança;
- Possuir capacidade de remontagem de pacotes para identificação de ataques;
- Deverá possuir capacidade de agrupar assinaturas para um determinado tipo de ataque; Exemplo: agrupar todas as assinaturas relacionadas a web-server para que seja usado para proteção específica de Servidores Web;
- Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep;
- Mecanismos de detecção/proteção de ataques;
- Reconhecimento de padrões;
- Análise de protocolos;
- Detecção de anomalias;
- Detecção de ataques de RPC (Remote procedure call);
- Proteção contra ataques de Windows ou NetBios;
- Proteção contra ataques de SMTP (Simple Message Transfer Protocol) IMAP (Internet Message Access Protocol, Sendmail ou POP (Post Office Protocol);
- Proteção contra ataques DNS (Domain Name System);
- Proteção contra ataques a FTP, SSH , Telnet e rlogin;
- Proteção contra ataques de ICMP (Internet Control Message Protocol);
- Alarmes na console de administração;
- Alertas via correio eletrônico;
- Monitoração do comportamento do appliance através de SNMP, o dispositivo deverá ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede;
- Capacidade de resposta/logs ativa a ataques;
- Terminação de sessões via TCP resets;
- Atualizar automaticamente as assinaturas para o sistema de detecção de intrusos;
- O Sistema de detecção de Intrusos deverá atenuar os efeitos dos ataques de negação de serviços;
- Possuir filtros de ataques por anomalias;
- Permitir filtros de anomalias de tráfego estatístico de: flooding, scan, source e destination session limit;
- Permitir filtros de anomalias de protocolos;
- Suportar reconhecimento de ataques de DoS, reconnaissance, exploits e evasion;
- Suportar verificação de ataque nas camadas de aplicação;

**3.3.1.7. DAS FUNCIONALIDADES DE QOS:**

- Adotar solução de Qualidade de Serviço baseada em appliance;
- Permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound) através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS;
- Permitir modificação de valores DSCP para o DiffServ;

- Limitar individualmente a banda utilizada por programas de compartilhamento de arquivos do tipo peer-to-peer;
- Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;
- Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP;
- Deverá controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP;
- Deverá controlar (limitar ou expandir) individualmente a banda utilizada por sub-rede de origem e destino;
- Deverá controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino;

**3.3.1.8. DAS FUNCIONALIDADES DO ANTIVÍRUS:**

- Possuir funções de Antivírus, Anti-spyware;
- Possuir antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, SMTP, POP3 e FTP;
- Permitir o bloqueio de malwares (adware, spyware, hijackers, keyloggers, etc.)
- Permitir o bloqueio de download de arquivos por extensão e tipo de arquivo;
- Permitir o bloqueio de download de arquivos por tamanho.

**3.3.1.9. DAS FUNCIONALIDADES DO PROXY E FILTRO DE CONTEÚDO WEB:**

- Possuir solução de filtro de conteúdo web integrado a solução de segurança
- Possuir pelo menos 75 categorias para classificação de sites web
- Possuir base mínima contendo, 40 milhões de sites internet web já registrados e classificados;
- Possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites web como:
- Webmail;
- Instituições de Saúde;
- Notícias;
- Pornografia;
- Restaurante;
- Mídias Sociais;
- Esporte;
- Educação;
- Games;
- Compras;
- Permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários;
- Integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados;
- Prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;
- Exibir mensagens de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança da contratante;
- Permitir a filtragem de todo o conteúdo do tráfego WEB de URLs conhecidas como fonte de material impróprio e códigos (programas/scripts) maliciosos em applets Java, cookies, activeX através de: base de URL própria atualizável;
- Permitir o bloqueio de páginas web através da construção de filtros específicos com mecanismo de busca textual;

- Permitir a criação de listas personalizadas de URLs permitidas – lista branca e bloqueadas – lista negra;
- Deverá permitir o bloqueio de URLs inválidas cujo campo CN do certificado SSL não contém um domínio válido;
- Garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo web;
- Deverá permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP;
- Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;
- Deverá permitir a criação de regras para acesso/bloqueio por sub-rede de origem;
- Deverá ser capaz de categorizar a página web tanto pela sua URL como pelo seu endereço IP;
- Deverá permitir o bloqueio de páginas web por Classificação como páginas que facilitam a busca de Audio, Video e URLs originadas de Spam;
- Deverá permitir a criação de listas personalizadas de URLs permitidas – lista branca e bloqueadas – lista negra;
- Deverá funcionar em modo Proxy Explícito para HTTP, HTTPS, e FTP e em Proxy Transparente;
- Deverá permitir configurar a porta do Proxy Explícito.

**3.3.1.10. DAS FUNCIONALIDADES DO CONTROLE DE APLICAÇÕES:**

- As funcionalidades abaixo devem ser baseadas em appliance:
- Deverá reconhecer no mínimo 700 aplicações;
- Deverá possuir pelo menos 10 categorias para classificação de aplicações;
- Deverá possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações como:
- P2P;
- Web;
- Transferência de arquivos;
- Chat;
- Social;
- Deverá permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários;
- Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;
- Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;
- Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory;
- Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP;
- Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;
- Deverá permitir a criação de regras para acesso/bloqueio por sub-rede de origem e destino;
- Deverá garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações.

**3.3.1.11. SISTEMA DE PROTEÇÃO AVANÇADA CONTRA AMEAÇAS – ATP:**

- Possuir sistema de proteção avançada contra ameaças (ATP) nativo;
- O sistema de ATP deve monitorar e analisar o tráfego da rede, identificar aplicativos e ameaças de ataques direcionados e persistentes e efetuar os respectivos bloqueios.
- Deve ser baseado em uma lista de assinaturas eletrônicas que atue em tempo real analisando a camada de aplicação, capaz de identificar o conteúdo dos pacotes, fazer log

(registros) das assinaturas trafegadas, inspecionar os pacotes e efetuar o descarte automático do pacote quando identificado assinaturas de pacotes maliciosos, inapropriados para o uso no ambiente corporativo;

- A base de assinaturas do sistema de ATP nativo deverá ser fornecida pelo período do contrato;
- Possuir um mínimo de 31 mil (trinta e um mil) assinaturas;
- Dever permitir a identificação de aplicativos e ameaças independente das portas e protocolos;
- Deve permitir a atualização automática das assinaturas por meio de agendamento diário;
- Possuir capacidade de inspecionar e bloquear em tempo real, ameaças do tipo: activex, malware, malware-backdoors, ataques P2P, trojans, worms, user_agents, pua (adware, p2p, toolbars) malwares para mobile, blacklist, botcc, exploits-kits, file-executable, file-flash, file-identify, file-image, file-java, file-multimedia, file-office, file-other, file-pdf, games, inappropriate e vulnerabilidades conhecidas;
- Possuir uma ferramenta de bloqueio de execução de aplicativos, integrado a base de Antivírus e Antimalware;
- Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos do tipo: ads, cloud, colaboração, download, e-mail, games, mobile, p2p, proxy, remote, redes sociais; storage, streaming, update, voip e web.
- Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos de VoIP tais como: Hotline, Asterisk, Linphone, SIP, Skype, Xlite SIP, X-Pro SIP, Cisco SIP, OpenSIP, Bria, ClearSea e Nero SIP;
- Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos de Redes Sociais tais como: Aol Instant Messenger, Badoo, BaiduHi, Airtime, Blogger, BoldChat, ChatON, China.com, Facebook, Flickr, FC2, Fring, Google Analytics, Google App, ICQ, Linkdin, Meetup, MSM Messenger, Netlog, Skype, Tinder, Tuenti, Twitter, WhatssApp, WeChat e Zoho Chat;
- Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos e transferências de arquivos do tipo P2P (peer to peer) tais como: BitTorrent, Gnutella, FastTrack, IceShare, Napster, Shareman e de Storages, tais como: Dropbox, Easy-share, Google Drive, Megashare, MegaUpload, Rapidshare, OneDrive, Yahoo Box, SoundCloud e Filemail, DivShare;
- Suportar exceção de ameaças por assinatura; IP de origem ou IP de destino;
- Suportar exceção de aplicativos por assinatura; IP de origem ou IP de destino;
- Deve possuir mecanismos para gerar gráfico do histórico da relação de eventos entre as “ameaças detectadas” e as “ameaças bloqueadas”;
- Deve possuir mecanismos para gerar gráfico do histórico da relação de eventos entre os “aplicativos detectados” e os “aplicativos bloqueados”;
- Deve possuir mecanismos para gerar log dos registros das incidências, classificados em pelo menos 3 (três) níveis de impacto: “baixo; médio e alto”;
- Gerar registro do tipo Top Level, dos 10(dez) mais, inclusive da relação de eventos entre usuários e ameaças, usuário e aplicativos, aplicativos e ameaças identificados e bloqueados;

**3.3.1.12. WAN DEFINIDA POR SOFTWARE - SD-WAN:**

- Possuir funcionalidades de SD-WAN, não se limitando aos recursos solicitados abaixo;
- Possuir o balanceamento automático para conexões externas à internet através das interfaces físicas;
- Permitir utilizar VPN IPsec para interligar unidades remotas;
- Possuir recurso de “persistência de link” para impedir a queda de conexões em aplicações que não suportam o load balance de link;

- O balanceamento deverá ser baseado em critérios de desempenho, devendo no mínimo, permitir verificar o monitoramento do consumo de banda, perda de pacotes, jitter e latência;
- Deve possuir uma janela web ou dashboard capaz de fornecer informações dos eventos relacionado ao recurso SD-WAN;
- Deverá oferecer um monitor capaz de prover em tempo real as seguintes informações:
- Consumo de banda;
- Perda de pacotes;
- Jitter;
- Latência.

**3.3.1.13. ALTA DISPONIBILIDADE:**

- Possuir mecanismo de Alta Disponibilidade operando em modo Ativo/Standby, com as implementações de Fail Over.
- Não serão permitidas soluções de cluster (HA) que façam com que o equipamento (s) reinicie após qualquer modificação de parâmetro/configuração seja realizada pelo administrador.
- O Sincronismo dos servidores deve ser por interface exclusiva permitindo utilizar mais de uma interface de Heartbeat;

**3.3.2. SERVIÇOS DE SUPORTE TÉCNICO REMOTO 14X6**

- Serviço de suporte REMOTO para os equipamentos de segurança de borda contratados, no horário 14X6(Segunda a sábado das 08:00 às 22:00, exceto feriados), pelo tempo de contrato, com as seguintes características:
- A contratada deve possuir serviço de abertura de chamados remoto capaz de abrir chamados de forma centralizada, em caso de ocorrências de defeitos e/ou falhas na rede relativos aos equipamentos e/ou produtos fornecidos;
- A contratada deverá iniciar o atendimento de suporte em no máximo 8 horas úteis após a abertura do chamado;
- A contratada deverá fornecer atestado comprovando a existência de equipe técnica de no mínimo 3 pessoas capacitadas em todas as soluções adquiridas. O atestado deverá ser fornecido pelo fabricante;
- A CONTRATADA será eximida da aplicação das sanções administrativas para os respectivos chamados em que sejam descumpridos os tempos de solução, desde que comprovadas as seguintes situações: Quando constatado que o problema está relacionado a “bug” no produto e que o fabricante não possui uma correção imediata para tal, sendo este fato declarado pelo próprio;
- A CONTRATADA tomou todas as medidas possíveis visando providenciar solução de contorno;

**3.3.3. SERVIÇOS DE INSTALAÇÃO**

- Para as soluções ofertadas, a contratada deverá cotar um valor total para a instalação e customização inicial dos dispositivos adquiridos;
- Este serviço deverá ser utilizado para a operacionalização inicial dos produtos adquiridos, customização, funcionalidades e políticas;
- A instalação deve ser feita por técnicos treinados e certificados, comprovados através de atestado emitido pelo fabricante;
- Toda a despesa de deslocamento e hospedagem deve ser de responsabilidade da contratada;
- O projeto de planejamento e execução das atividades de instalação e configuração deverão ser assinadas por um profissional com certificação em gerenciamento de projetos - PMP (Project Management Professional);

- A CONTRATADA deverá apresentar o certificado PMP válido no momento da assinatura do contato e o profissional deverá ser registrado com carteira assinada;
- Caso a CONTRATADA não possua um profissional com certificação PMP será necessário que o FABRICANTE da solução ofertada tenha em seu quadro de funcionários residente no Brasil, o profissional PMP e este deverá assinar o projeto de planejamento e execução da revenda autorizada.

**3.3.4.** SUBSCRIÇÃO PARA ATUALIZAÇÃO DE BASE DE CONHECIMENTO

- Atualização da base de conhecimento de antimalware pelo período de contrato;
- Atualização da base de conhecimento de IPS pelo período de contrato;
- Atualização da base de conhecimento de ATP pelo período de contrato;
- Atualização da base de conhecimento de Aplicativos pelo período de contrato;
- Atualização da base de conhecimento de filtro de conteúdo WEB pelo período de contrato.

## 3.4. ITEM 4: AQUISIÇÃO BB10 SPARE

### 3.4.1. CARACTERÍSTICAS DO HARDWARE

- O equipamento deve se instalar em mesa ocupando no máximo 1U (44,45mm) da referida mesa;
- Dispor de fonte de alimentação com tensão de entrada de 110V / 220V AC automática e frequência de 50-60 Hz;
- Deverão ser fornecidos todos os cabos de energia, serial (RS-232/RJ45), para instalação e funcionamento do dispositivo;
- Possuir led indicador on/off, disco e devices de rede;
- Possuir throughput mínimo de 2000 Mbps para tráfego UDP;
- Suportar no mínimo 250.000 (duzentas e cinquenta mil) conexões simultâneas;
- Suportar no mínimo 17.000 (Dezessete mil) novas conexões por segundo;
- Possuir throughput mínimo de 450 Mbps para tráfego HTTP/ HTTPS via Proxy;
- Possuir throughput mínimo de 175 Mbps para tráfego HTTP/ HTTPS com inspeção SSL via Proxy;
- Possuir throughput mínimo de 260 Mbps para tráfego IPS;
- Possuir throughput mínimo de 335 Mbps para tráfego VPN IPSEC com criptografia (AES-128);
- Possuir throughput mínimo de 210 Mbps para tráfego VPN SSL com criptografia (AES-128);
- Possuir no mínimo 4 (quatro) interfaces de rede Gigabit Ethernet 10/100/1000 com leds indicativos de link e atividade, as portas entregues deverão ser roteáveis, ou seja, não será aceito equipamento com porta do tipo switch;
- Possuir dispositivo de armazenamento interno de no mínimo 32 GB padrão SSD;
- Possuir no mínimo 1 (uma) porta console de conexão padrão RJ45 para acesso a interface de comando CLI específica para esta finalidade, utilizando cabo do tipo serial RS-232/RJ-45;
- Possuir pelo menos 1 (uma) portas USB para conexão de dispositivos externos.

### 3.4.2. ESPECIFICAÇÕES GERIAS DE SOFTWARE UTM SPARE:

- O equipamento spare deverá permitir a instalação do software de Firewall UTM especificado no ITEM 3.

## 3.5. ITEM 5: AQUISIÇÃO BB 50

### 3.5.1. CARACTERÍSTICAS DO HARDWARE

- O equipamento deve se instalar em rack com largura padrão de 19 polegadas, padrão EIA-310, ocupando no máximo 1U (44,45mm) do referido rack;

- Dispor de fonte de alimentação interna com tensão de entrada de 110V / 220V AC automática e frequência de 50-60 Hz;
- Possuir painel/led indicador on/off, disco e devices de rede;
- Possuir throughput de no mínimo 4000 Mbps para tráfego UDP;
- Suportar no mínimo 500.000 (quinhentas mil) conexões simultâneas;
- Suportar no mínimo 35.000 (trinta e cinco mil) novas conexões por segundo;
- Possuir throughput de no mínimo 720 Mbps para tráfego HTTP/ HTTPS via proxy;
- Possuir throughput de no mínimo 280 Mbps para tráfego HTTP/ HTTPS com inspeção SSL via proxy;
- Possuir throughput de no mínimo 369 Mbps para tráfego IPS;
- Possuir throughput de no mínimo 584 Mbps para tráfego VPN IPSEC com criptografia (AES-128);
- Possuir throughput de no mínimo 485 Mbps para tráfego VPN SSL com criptografia (AES-128);
- Possuir pelo menos 6 (seis) interfaces de rede Gigabit Ethernet 10/100/1000 com leds indicativos de link e atividade, as portas entregues deverão ser roteáveis, ou seja, não será aceito equipamento com porta do tipo switch;
- Possuir dispositivo de armazenamento interno de no mínimo 120 GB padrão SSD;
- Possuir no mínimo 1 (uma) porta console de conexão padrão RJ45 para acesso a interface de comando CLI específica para esta finalidade, utilizando cabo do tipo serial RS-232/RJ-45;
- Possuir no mínimo 2 (duas) portas USB para conexão de dispositivos externos;

### 3.5.2. ESPECIFICAÇÕES GERIAS DE SOFTWARE UTM

#### 3.5.2.1. FUNÇÕES BÁSICAS:

- Hardware (Appliances) que atuam na segurança e performance do ambiente de rede;
- VPN SSL, VPN IPSec (Client-to-site e Site-to-site);
- Controle de Aplicações;
- Proxy Web e Filtro de Conteúdo Web (URL Filtering);
- Detecção e prevenção de intrusos – IPS;
- Qualidade de serviço – QOS;
- Anti-Malware;
- SD-WAN;
- Cluster.

#### 3.5.2.2. CARACTERÍSTICAS GERAIS:

- A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
- Interface em português e inglês;
- O sistema deve permitir o acesso à interface de gerenciamento WEB por qualquer interface de rede configurada;
- O software deverá ser fornecido em sua versão mais atualizada, não sendo permitido qualquer tipo de comprovação futura.
- Todo o ambiente deverá ser gerenciado sem a necessidade de produtos de terceiros para compor a solução.
- Tanto os Gateways de Segurança bem como a Gerência Centralizada deverão suportar monitoramento através de SNMP v1, v2 e v3.
- A Solução deverá prover inspeção SSL:
- A solução deverá ser em hardware dedicado tipo appliance com sistema operacional customizado para garantir segurança e melhor desempenho.

- Deve ser totalmente gerenciável remotamente, através de rede local, sem a necessidade de instalação de mouse, teclado e monitor de vídeo;
- Deve suportar cluster do tipo Failover (HA) com replicação da tabela de estado.

**3.5.2.3. DAS FUNCIONALIDADES DO FIREWALL:**

- Possuir capacidade de processamento de pacotes e interfaces de acordo com a tabela de performance dos equipamentos;
- Permitir a conexão simultânea de vários administradores, com poderes de alteração de configurações e/ou apenas de visualização das mesmas;
- Possuir um sistema de armazenamento remoto para salvar backups da solução com suporte a conexões do tipo Network File System, SSH e PenDrive;
- Possibilitar a visualização dos países de origem e destino nos logs de eventos, de acessos e ameaças.
- Possuir mecanismo que permita a realização de cópias de segurança (backups) do sistema e restauração remota, através da interface gráfica, a solução deve permitir o agendamento diário ou semanal;
- O sistema deve permitir configurar o período ou número de cópias que deseja manter no repositório remoto e executar a manutenção de período automaticamente.
- As cópias de segurança devem ser salvas compactadas e criptografadas de forma a garantir segurança, confiabilidade e confidencialidade dos arquivos de backup;
- O sistema ainda deve contemplar um recurso de cópia de segurança do tipo snapshot, que contemple a cópia completa das configurações dos serviços e recursos do sistema;
- Deve possibilitar a restauração do snapshot através da interface web de qualquer ponto remoto, de modo a contribuir para uma restauração imediata sem a necessidade de reinicialização do sistema;
- Deve permitir habilitar ou desabilitar o registro de log por política de firewall.
- Possuir controle de acesso à internet por endereço IP de origem e destino;
- Possuir controle de acesso à internet por sub-rede;
- Possuir suporte a tags de VLAN (802.1q);
- Suportar agregação de links, segundo padrão IEEE 802.3ad;
- Possuir ferramenta de diagnóstico do tipo tcpdump;
- Possuir integração com Servidores de Autenticação RADIUS, TACACS+, LDAP e Microsoft Active Directory;
- Possuir métodos de autenticação de usuários para qualquer aplicação que se execute sob os protocolos TCP ( HTTP, HTTPS, FTP e Telnet);
- Possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation), um para um, N-para-um e vários para um.
- Permitir controle de acesso à internet por períodos do dia, permitindo a aplicação de políticas por horários e por dia da semana;
- Permitir controle de acesso à internet por domínio, exemplo: gov.br, org.br, edu.br;
- Possuir a funcionalidade de fazer tradução de endereços dinâmicos, muitos para um, PAT.
- Possuir suporte a roteamento dinâmico RIP V1, V2, OSPF, BGP;
- Possuir funcionalidades de DHCP Cliente, Servidor e Relay;
- Deverá suportar aplicações multimídia como: H.323, SIP;
- Possuir tecnologia de firewall do tipo Stateful;
- Possuir alta disponibilidade (HA), trabalhando no esquema de redundância do tipo ativo-passivo;
- Permitir o funcionamento em modo transparente tipo “bridge”;
- Permitir a criação de pelo menos 20 VLANS no padrão IEEE 802.1q;
- Possuir conexão entre estação de gerência e appliance criptografada tanto em interface gráfica quanto em CLI (linha de comando);

- Deverá suportar forwarding de multicast;
- Permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos, TCP, UDP, ICMP e IP;
- Permitir o agrupamento de serviços;
- Permitir o filtro de pacotes sem a utilização de NAT;
- Permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas;
- Possuir mecanismo de anti-spoofing;
- Permitir criação de regras definidas pelo usuário;
- Permitir o serviço de autenticação para HTTP e FTP;
- Possuir a funcionalidade de balanceamento e contingência de links;
- Deverá ter técnicas de detecção de programas de compartilhamento de arquivos (peer-to-peer) e de mensagens instantâneas, suportando ao menos: Yahoo! Messenger, MSN Messenger, ICQ, AOL Messenger, BitTorrent, eDonkey, GNUTella, KaZaa, Skype e WinNY.

**3.5.2.4. IDENTIFICAÇÃO DE USUÁRIO:**

- Deve possuir a capacidade de criação de políticas de acesso de Firewall, VPN, IPS e Controle de aplicação integradas ao repositório de usuários sendo: Active Directory, LDAP, TACAC´S e Radius;
- Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- Para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador (Captive Portal), sem a necessidade de agente;
- Deve possuir Captive Portal com suporte a Autenticação Social (Facebook, Twitter, Google);
- A solução deverá ser capaz de identificar nome do usuário, login, máquina/computador registrados no Microsoft Active Directory;
- Na integração com o AD, todos os domain controllers em operação na rede do cliente devem ser cadastrados de maneira simples e sem utilização de scritps de comando;
- A solução de identificação de usuário deverá se integrar com as funcionalidades Firewall, controle de aplicação e IPS, sendo elas do mesmo fabricante;
- A solução deve suportar a opção de instalação de softwares agentes nos PCs/Laptops para que os próprios PCs/Laptops enviem suas credenciais de IP/nome de usuário do domínio/nome da máquina para o gateway diretamente, sem que o Gateway tenha que fazer Queries no AD;

**3.5.2.5. DAS FUNCIONALIDADES DA VPN:**

- VPN baseada em appliance;
- Possuir algoritmos de criptografia para túneis VPN: AES, DES, 3DES;
- Suporte a certificados PKI X.509 para construção de VPNs;
- Possuir suporte a VPNs IPSec site-to-site:
- Criptografia, 3DES, AES128, AES256, AES-GCM-128
- Integridade MD5, SHA-1, SHA-256, SHA384 e AES-XCBC;
- Algoritmo Internet Key Exchange (IKE) versões I e II;
- AES 128 e 256 (Advanced Encryption Standard);
- Suporte a Diffie-Hellman Grupo 1, Grupo 2, Grupo 5, Grupo 14; Grupo 15, Grupo 16, Grupo 17, Grupo 18, Grupo 19, Grupo 20, Grupo 21, Grupo 22, Grupo 23, Grupo 24, Grupo 25, Grupo 26, Grupo 27, Grupo 28, Grupo 29, Grupo 30;
- Possuir suporte a VPN SSL;
- Possuir capacidade de realizar SSL VPNs utilizando certificados digitais;

- A VPN SSL deve possibilitar o acesso a toda infra-estrutura da contratante de acordo com a política de segurança, através de um plug-in ActiveX e/ou Java;
- Deve permitir a arquitetura de vpn hub and spoke;
- Suporte a VPNs IPSec client-to-site;
- Deverá possuir cliente próprio para Windows para o estabelecimento da VPN client-to-site.
- Suporte à inclusão em autoridades certificadoras (enrollment) mediante SCEP (Simple Certificate Enrollment Protocol);
- Possuir funcionalidades de Auto-Dicovery VPN capaz de permitir criar tuneis de VPN dinâmicos entre múltiplos dispositivos (spokes) com um gateway centralizador (hub).;
- A funcionalidade de AD-VPN deve suportar criar os seguintes tipos de tuneis:
- Site-to-Site;
- Full-Mesh;
- Star.

**3.5.2.6. DAS FUNCIONALIDADES DA DETECÇÃO DE INTRUSÃO:**

- A Detecção de Intrusão deverá ser baseada em appliance:
- Capacidade de detecção de mais de 22.000 ataques;
- O Sistema de detecção e proteção de intrusão deverá estar orientado à proteção de redes;
- Possuir tecnologia de detecção baseada em assinatura;
- O sistema de detecção e proteção de intrusão deverá possuir integração à plataforma de segurança;
- Possuir capacidade de remontagem de pacotes para identificação de ataques;
- Deverá possuir capacidade de agrupar assinaturas para um determinado tipo de ataque; Exemplo: agrupar todas as assinaturas relacionadas a web-server para que seja usado para proteção específica de Servidores Web;
- Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep;
- Mecanismos de detecção/proteção de ataques;
- Reconhecimento de padrões;
- Análise de protocolos;
- Detecção de anomalias;
- Detecção de ataques de RPC (Remote procedure call);
- Proteção contra ataques de Windows ou NetBios;
- Proteção contra ataques de SMTP (Simple Message Transfer Protocol) IMAP (Internet Message Access Protocol, Sendmail ou POP (Post Office Protocol);
- Proteção contra ataques DNS (Domain Name System);
- Proteção contra ataques a FTP, SSH , Telnet e rlogin;
- Proteção contra ataques de ICMP (Internet Control Message Protocol);
- Alarmes na console de administração;
- Alertas via correio eletrônico;
- Monitoração do comportamento do appliance através de SNMP, o dispositivo deverá ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede;
- Capacidade de resposta/logs ativa a ataques;
- Terminação de sessões via TCP resets;
- Atualizar automaticamente as assinaturas para o sistema de detecção de intrusos;
- O Sistema de detecção de Intrusos deverá atenuar os efeitos dos ataques de negação de serviços;
- Possuir filtros de ataques por anomalias;
- Permitir filtros de anomalias de tráfego estatístico de: flooding, scan, source e destination session limit;

- Permitir filtros de anomalias de protocolos;
- Suportar reconhecimento de ataques de DoS, reconnaissance, exploits e evasion;
- Suportar verificação de ataque nas camadas de aplicação;

**3.5.2.7. DAS FUNCIONALIDADES DE QOS:**

- Adotar solução de Qualidade de Serviço baseada em appliance;
- Permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound) através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS;
- Permitir modificação de valores DSCP para o DiffServ;
- Limitar individualmente a banda utilizada por programas de compartilhamento de arquivos do tipo peer-to-peer;
- Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;
- Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP;
- Deverá controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP;
- Deverá controlar (limitar ou expandir) individualmente a banda utilizada por sub-rede de origem e destino;
- Deverá controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino;

**3.5.2.8. DAS FUNCIONALIDADES DO ANTIVÍRUS:**

- Possuir funções de Antivírus, Anti-spyware;
- Possuir antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, SMTP, POP3 e FTP;
- Permitir o bloqueio de malwares (adware, spyware, hijackers, keyloggers, etc.)
- Permitir o bloqueio de download de arquivos por extensão e tipo de arquivo;
- Permitir o bloqueio de download de arquivos por tamanho.

**3.5.2.9. DAS FUNCIONALIDADES DO PROXY E FILTRO DE CONTEÚDO WEB:**

- Possuir solução de filtro de conteúdo web integrado a solução de segurança
- Possuir pelo menos 75 categorias para classificação de sites web
- Possuir base mínima contendo, 40 milhões de sites internet web já registrados e classificados;
- Possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites web como:
- Webmail;
- Instituições de Saúde;
- Notícias;
- Pornografia;
- Restaurante;
- Mídias Sociais;
- Esporte;
- Educação;
- Games;
- Compras;
- Permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários;
- Integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados;

- Prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;
- Exibir mensagens de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança da contratante;
- Permitir a filtragem de todo o conteúdo do tráfego WEB de URLs conhecidas como fonte de material impróprio e códigos (programas/scripts) maliciosos em applets Java, cookies, activeX através de: base de URL própria atualizável;
- Permitir o bloqueio de páginas web através da construção de filtros específicos com mecanismo de busca textual;
- Permitir a criação de listas personalizadas de URLs permitidas – lista branca e bloqueadas – lista negra;
- Deverá permitir o bloqueio de URLs inválidas cujo campo CN do certificado SSL não contém um domínio válido;
- Garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo web;
- Deverá permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP;
- Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;
- Deverá permitir a criação de regras para acesso/bloqueio por sub-rede de origem;
- Deverá ser capaz de categorizar a página web tanto pela sua URL como pelo seu endereço IP;
- Deverá permitir o bloqueio de páginas web por Classificação como páginas que facilitam a busca de Audio, Video e URLs originadas de Spam;
- Deverá permitir a criação de listas personalizadas de URLs permitidas – lista branca e bloqueadas – lista negra;
- Deverá funcionar em modo Proxy Explícito para HTTP, HTTPS, e FTP e em Proxy Transparente;
- Deverá permitir configurar a porta do Proxy Explícito.

**3.5.2.10. DAS FUNCIONALIDADES DO CONTROLE DE APLICAÇÕES:**

- As funcionalidades abaixo devem ser baseadas em appliance:
- Deverá reconhecer no mínimo 700 aplicações;
- Deverá possuir pelo menos 10 categorias para classificação de aplicações;
- Deverá possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações como:
- P2P;
- Web;
- Transferência de arquivos;
- Chat;
- Social;
- Deverá permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários;
- Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;
- Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;
- Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory;
- Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP;
- Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;

- Deverá permitir a criação de regras para acesso/bloqueio por sub-rede de origem e destino;
- Deverá garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações.

**3.5.2.11. SISTEMA DE PROTEÇÃO AVANÇADA CONTRA AMEAÇAS – ATP:**

- Possuir sistema de proteção avançada contra ameaças (ATP) nativo;
- O sistema de ATP deve monitorar e analisar o tráfego da rede, identificar aplicativos e ameaças de ataques direcionados e persistentes e efetuar os respectivos bloqueios.
- Deve ser baseado em uma lista de assinaturas eletrônicas que atue em tempo real analisando a camada de aplicação, capaz de identificar o conteúdo dos pacotes, fazer log (registros) das assinaturas trafegadas, inspecionar os pacotes e efetuar o descarte automático do pacote quando identificado assinaturas de pacotes maliciosos, inapropriados para o uso no ambiente corporativo;
- A base de assinaturas do sistema de ATP nativo deverá ser fornecida pelo período do contrato;
- Possuir um mínimo de 31 mil (trinta e um mil) assinaturas;
- Dever permitir a identificação de aplicativos e ameaças independente das portas e protocolos;
- Deve permitir a atualização automática das assinaturas por meio de agendamento diário;
- Possuir capacidade de inspecionar e bloquear em tempo real, ameaças do tipo: activex, malware, malware-backdoors, ataques P2P, trojans, worms, user_agents, pua (adware, p2p, toolbars) malwares para mobile, blacklist, botcc, exploits-kits, file-executable, file-flash, file-identify, file-image, file-java, file-multimedia, file-office, file-other, file-pdf, games, inappropriate e vulnerabilidades conhecidas;
- Possuir uma ferramenta de bloqueio de execução de aplicativos, integrado a base de Antivírus e Antimalware;
- Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos do tipo: ads, cloud, colaboração, download, e-mail, games, mobile, p2p, proxy, remote, redes sociais; storage, streaming, update, voip e web.
- Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos de VoIP tais como: Hotline, Asterisk, Linphone, SIP, Skype, Xlite SIP, X-Pro SIP, Cisco SIP, OpenSIP, Bria, ClearSea e Nero SIP;
- Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos de Redes Sociais tais como: Aol Instant Messenger, Badoo, BaiduHi, Airtime, Blogger, BoldChat, ChatON, China.com, Facebook, Flickr, FC2, Fring, Google Analytics, Google App, ICQ, Linkdin, Meetup, MSM Messenger, Netlog, Skype, Tinder, Tuenti, Twitter, WhatssApp, WeChat e Zoho Chat;
- Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos e transferências de arquivos do tipo P2P (peer to peer) tais como: BitTorrent, Gnutella, FastTrack, IceShare, Napster, Shareman e de Storages, tais como: Dropbox, Easy-share, Google Drive, Megashare, MegaUpload, Rapidshare, OneDrive, Yahoo Box, SoundCloud e Filemail, DivShare;
- Suportar exceção de ameaças por assinatura; IP de origem ou IP de destino;
- Suportar exceção de aplicativos por assinatura; IP de origem ou IP de destino;
- Deve possuir mecanismos para gerar gráfico do histórico da relação de eventos entre as “ameaças detectadas” e as “ameaças bloqueadas”;
- Deve possuir mecanismos para gerar gráfico do histórico da relação de eventos entre os “aplicativos detectados” e os “aplicativos bloqueados”;
- Deve possuir mecanismos para gerar log dos registros das incidências, classificados em pelo menos 3 (três) níveis de impacto: “baixo; médio e alto”;

- Gerar registro do tipo Top Level, dos 10(dez) mais, inclusive da relação de eventos entre usuários e ameaças, usuário e aplicativos, aplicativos e ameaças identificados e bloqueados;

**3.5.2.12. WAN DEFINIDA POR SOFTWARE - SD-WAN:**

- Possuir funcionalidades de SD-WAN, não se limitando aos recursos solicitados abaixo;
- Possuir o balanceamento automático para conexões externas à internet através das interfaces físicas;
- Permitir utilizar VPN IPsec para interligar unidades remotas;
- Possuir recurso de "persistência de link" para impedir a queda de conexões em aplicações que não suportam o load balance de link;
- O balanceamento deverá ser baseado em critérios de desempenho, devendo no mínimo, permitir verificar o monitoramento do consumo de banda, perda de pacotes, jitter e latência;
- Deve possuir uma janela web ou dashboard capaz de fornecer informações dos eventos relacionado ao recurso SD-WAN;
- Deverá oferecer um monitor capaz de prover em tempo real as seguintes informações:
- Consumo de banda;
- Perda de pacotes;
- Jitter;
- Latência.

**3.5.2.13. ALTA DISPONIBILIDADE:**

- Possuir mecanismo de Alta Disponibilidade operando em modo Ativo/Standby, com as implementações de Fail Over.
- Não serão permitidas soluções de cluster (HA) que façam com que o equipamento (s) reinicie após qualquer modificação de parâmetro/configuração seja realizada pelo administrador.
- O Sincronismo dos servidores deve ser por interface exclusiva permitindo utilizar mais de uma interface de Heartbeat;

**3.5.3. SUBSCRIÇÃO PARA ATUALIZAÇÃO DE BASE DE CONHECIMENTO:**

- Atualização da base de conhecimento de antimalware pelo período de contrato;
- Atualização da base de conhecimento de IPS pelo período de contrato;
- Atualização da base de conhecimento de ATP pelo período de contrato;
- Atualização da base de conhecimento de Aplicativos pelo período de contrato;
- Atualização da base de conhecimento de filtro de conteúdo WEB pelo período de contrato;

**3.5.4. SERVIÇOS DE SUPORTE TÉCNICO REMOTO 14X6:**

- Serviço de suporte REMOTO para os equipamentos de segurança de borda contratados, no horário 14X6(Segunda a sábado das 08:00 às 22:00, exceto feriados), pelo tempo de contrato, com as seguintes características:
- A contratada deve possuir serviço de abertura de chamados remoto capaz de abrir chamados de forma centralizada, em caso de ocorrências de defeitos e/ou falhas na rede relativos aos equipamentos e/ou produtos fornecidos;
- A contratada deverá iniciar o atendimento de suporte em no máximo 8 horas úteis após a abertura do chamado;
- A contratada deverá fornecer atestado comprovando a existência de equipe técnica de no mínimo 3 pessoas capacitadas em todas as soluções adquiridas. O atestado deverá ser fornecido pelo fabricante;
- A CONTRATADA será eximida da aplicação das sanções administrativas para os respectivos chamados em que sejam descumpridos os tempos de solução, desde que

comprovadas as seguintes situações: Quando constatado que o problema está relacionado a “bug” no produto e que o fabricante não possui uma correção imediata para tal, sendo este fato declarado pelo próprio;

- A CONTRATADA tomou todas as medidas possíveis visando providenciar solução de contorno.

**3.5.5. SERVIÇOS DE INSTALAÇÃO:**

- Para as soluções ofertadas, a contratada deverá cotar um valor total para a instalação e customização inicial dos dispositivos adquiridos;
- Este serviço deverá ser utilizado para a operacionalização inicial dos produtos adquiridos, customização, funcionalidades e políticas;
- A instalação deve ser feita por técnicos treinados e certificados, comprovados através de atestado emitido pelo fabricante;
- Toda a despesa de deslocamento e hospedagem deve ser de responsabilidade da contratada;
- O projeto de planejamento e execução das atividades de instalação e configuração deverão ser assinadas por um profissional com certificação em gerenciamento de projetos - PMP (Project Management Professional);
- A CONTRATADA deverá apresentar o certificado PMP válido no momento da assinatura do contato e o profissional deverá ser registrado com carteira assinada;
- Caso a CONTRATADA não possua um profissional com certificação PMP será necessário que o FABRICANTE da solução ofertada tenha em seu quadro de funcionários residente no Brasil, o profissional PMP e este deverá assinar o projeto de planejamento e execução da revenda autorizada.

## 4. DA CLASSIFICAÇÃO DOS SERVIÇOS E FORMA DE SELEÇÃO DO FORNECEDOR:

**4.1.** Trata-se de serviço comum, não continuado, a ser contratado mediante licitação, na modalidade pregão, em sua forma eletrônica.

**4.2.** Os serviços a serem contratados enquadram-se nos pressupostos do Decreto Estadual n. 14.483, de 26 de maio de 2011, não se constituindo em quaisquer das atividades, previstas no art. 3º do aludido decreto, cuja execução indireta é vedada.

**4.3.** A prestação dos serviços não gera vínculo empregatício entre os empregados da Contratada e a Administração Contratante, vedando-se qualquer relação entre estes que caracterize pessoalidade e subordinação direta.

## 5. DOS RESQUISITOS DE CONTRATAÇÃO

**5.1.** A empresa adjudicada deverá manter as condições de habilitação obtidas na licitação para fins de assinatura do contrato.

**5.2.** O Contrato será assinado e firmado entre as partes interessadas através do sistema eletrônico SEI-PI, devendo a empresa adjudicada ser registrada através de disponibilização de link de acesso pela SEDUC-PI.

**5.3.** Os serviços serão executados conforme as etapas constantes no cronograma de execução a seguir:

| **ITEM 1: RENOVAÇÃO BB 10** | | |
|---|---|---|
| **ITEM** | **DESCRIÇÃO** | **PRAZO DE EXECUÇÃO** |
| 1.1 | Standard Software License - UTM Subscription - APL BB 10 - for 36 months | MÊS 01 |
| 1.2 | Suporte 14x6 - Banco de Horas Mensal - 3hrs - | 36 MESES (CORRESPONDE A |

| | | |
|---|---|---|
| | for 36 months | TODA VIGÊNCIA CONTRATUAL) |
| **ITEM 2: RENOVAÇÃO BB 10000** | | |
| **ITEM** | **DESCRIÇÃO** | **PRAZO DE EXECUÇÃO** |
| 2.1 | Standard Software License - UTM Subscription Advanced - APL BB 10000 - for 36 months | MÊS 02 |
| 2.2 | Suporte 14x6 - Banco de Horas Mensal - 3hrs - for 36 months | 36 MESES (CORRESPONDE A TODA VIGÊNCIA CONTRATUAL) |
| **ITEM 3: AQUISIÇÃO BB 10** | | |
| **ITEM** | **DESCRIÇÃO** | **PRAZO DE EXECUÇÃO** |
| 3.1 | Hardware Appliance APL UTM BB 10 | MÊS 03 |
| 3.2 | Standard Software License - APL UTM BB 10 | |
| 3.3 | Standard Software License - UTM Subscription - APL BB 10 - for 36 months | |
| 3.4 | Suporte 14x6 - Banco de Horas Mensal - 3hrs - for 36 months | 36 MESES (CORRESPONDE A TODA VIGÊNCIA CONTRATUAL) |
| 3.5 | Serviço de instalação | MÊS 03 E 04 |
| **ITEM 4: AQUISIÇÃO BB 10 SPARE** | | |
| **ITEM** | **DESCRIÇÃO** | **PRAZO DE EXECUÇÃO** |
| 4.1 | Hardware Appliance APL UTM BB 10 - Spare | MÊS 05 |
| 4.2 | Sistema Operacional Spare - APL UTM BB 10 | |
| **ITEM 5: AQUISIÇÃO BB 50** | | |
| **ITEM** | **DESCRIÇÃO** | **PRAZO DE EXECUÇÃO** |
| 5.1 | Hardware Appliance APL UTM BB 50 | MÊS 06 |
| 5.2 | Standard Software License - APL UTM BB 50 | |
| 5.3 | Standard Software License - UTM Subscription - APL BB 50 - for 36 months | |
| 5.4 | Suporte 14x6 - Banco de Horas Mensal - 3hrs - for 36 months | 36 MESES (CORRESPONDE A TODA VIGÊNCIA CONTRATUAL) |
| 5.5 | Serviço de instalação | MÊS 06 E 07 |

**5.4.** O local de realização dos serviços será das 08h às 14h, na cidade de Teresina, PI, na Av. Pedro Freitas, S/N - Bloco D/F - Centro Administrativo., CEP 64.018-900, quando não puder ser realizado remotamente.

## 6. VISTORIA PARA A LICITAÇÃO

**6.1.** Para o correto dimensionamento e elaboração de sua proposta, o licitante poderá realizar vistoria nas instalações do local de execução dos serviços, acompanhado por servidor designado para esse fim, de segunda à sexta-feira, das 10 horas às 16 horas.

**6.2.** O prazo para vistoria iniciar-se-á no dia útil seguinte ao da publicação do Edital, estendendo-se até o dia útil anterior à data prevista para a abertura da sessão pública.

**6.2.1.** Para a vistoria o licitante, ou o seu representante legal, deverá estar devidamente identificado, apresentando documento de identidade civil e documento expedido pela empresa comprovando sua habilitação para a realização da vistoria.

**6.3.** Por ocasião da vistoria, ao licitante, ou ao seu representante legal, poderá ser entregue CD-ROM, “pen-drive” ou outra forma compatível de reprodução, contendo as informações relativas ao objeto da licitação, para que a empresa tenha condições de bem elaborar sua proposta.

**6.4.** A não realização da vistoria, quando facultativa, não poderá embasar posteriores alegações de desconhecimento das instalações, dúvidas ou esquecimentos de quaisquer detalhes dos locais da prestação dos serviços, devendo a licitante vencedora assumir os ônus dos serviços decorrentes.

**6.5.** A licitante deverá declarar que tomou conhecimento de todas as informações e das condições locais para o cumprimento das obrigações objeto da licitação.

## 7. MODELO DE EXECUÇÃO DO OBJETO

**7.1.** A execução do objeto seguirá a seguinte dinâmica:

**7.1.1.** Renovação de licenças do parque de equipamentos de segurança já existentes e expansão tecnológico de Firewall

**7.2.** Prazos e condições:

**7.2.1.** A CONTRATADA deverá fornecer, instalar e testar o funcionamento da solução no prazo de 60 dias, a contar da assinatura do contrato;

**7.2.2.** É marco intermediário para a entrega da solução:

**7.2.3.** Até 50 dias da assinatura do contrato para a entrega dos equipamentos e licenças a serem instalados.

**7.2.4.** Em até 10 dias da assinatura do contrato, a CONTRATADA deverá entrar em contato como o Gestor do contrato para apresentar o cronograma de trabalho para fornecimento da solução contratada.

**7.2.5.** O cronograma de trabalho deverá prever a logística de implementação definindo datas para a instalação e configuração, bem como o treinamento a ser realizado, para garantir a entrega da solução nos prazos estipulados.

**7.2.6.** 4.Indicar os dias que os profissionais atuarão nas dependências da SEDUC-PI.

**7.2.7.** 4. Qualquer alteração nos dias e horários de atuação deve ser informada com o Gestor do contrato com no mínimo 1 (um) dia útil de antecedência.

## 8. MODELO DE GESTÃO DO CONTRATO E CRITÉRIOS DE MEDIÇÃO:

**8.1.** Critérios de Aceitação:

**8.1.1.** Serão realizadas consultas diretamente no site do fabricante do equipamento, inclusive em manuais e toda documentação pública disponível para comprovação do pleno atendimento aos requisitos deste Termo de Referência. Em caso de dúvidas ou divergência na comprovação da especificação técnica, a SEDUC/PI poderá solicitar uma amostra do equipamento ofertado, sem ônus ao processo, para comprovação técnica de funcionalidades. Esta amostra deverá ocorrer em até 15 (quinze) dias úteis após a solicitação deste órgão. Para a amostra, a empresa deverá apresentar o mesmo modelo do equipamento ofertado no certame, com técnicos certificados na solução para configuração e comprovação dos itens pendentes, nas dependências do CPD/SEDUC/PI.

**8.1.2.** Os produtos serão inspecionados no ato da entrega, no CPD/SEDUC/PI, afim de verificar a conformidade, quantidade e realizar a inspeção visual da solução. Somente serão aceitos equipamentos novos e sem uso. Não serão aceitos equipamentos usados ou de demonstração. Os equipamentos deverão ser entregues nas caixas lacradas pelo fabricante, não sendo aceitos equipamentos com caixas violadas.

**8.1.3.** A existência de inspeção não isenta a contratada da responsabilidade pela qualidade do material fornecido.

**8.1.4.** A solução será recebida provisoriamente por uma equipe designada pelo Diretor do Centro de Processamento de Dados acompanhados dos fiscais do contrato a fim de permitir a realização dos testes e inspeção descritos no item

**8.1.5.** O aceite do bem e recebimento definitivo somente será dado após comprovação da entrega e o efetivo cumprimento de todas as exigências da presentes neste Termo de Referência e após aprovação no teste descrito no item 7.2.

**8.1.6.** O processo de implantação deverá ser devidamente documentado pela Contratada, que deverá apresentar relatório com o detalhamento do processo realizado ao final da implantação como requisito para o aceite definitivo.

**8.1.7.** O aceite do bem e recebimento definitivo somente será dado após comprovação da entrega e o efetivo cumprimento de todas as exigências da presentes neste Termo de Referência e após aprovação no teste descrito no item 7.2.

**8.1.8.** O processo de implantação deverá ser devidamente documentado pela Contratada, que deverá apresentar relatório com o detalhamento do processo realizado ao final da implantação como requisito para o aceite definitivo.

**8.1.9.** O aceite do serviço somente será dado após comprovação da instalação e o efetivo cumprimento de todas as configurações necessárias para funcionamento do equipamento dentro da estrutura da SEDUC/PI, como, por exemplo, a migração das regras de firewall existentes.

**8.1.10.** O aceite do serviço somente será dado após a apresentação de todos os conteúdos esperados e da resolução de possíveis dúvidas da equipe em treinamento.

**8.1.11.** Caso seja verificada alguma inconformidade na aceitação inicial do objeto, a Contratante informará à Contratada os motivos da não aceitação, devolvendo o(s) bem(ns) para correção.

**8.1.12.** Caberá à Contratada sanar as irregularidades identificadas na entrega dos bens, inclusive, substituí-los no prazo de 15 (quinze) dias da notificação, às suas expensas, quando fornecidos com problemas, apresentados fora das especificações técnicas estabelecidas, sob pena de incorrer nas sanções legais cabíveis.

**8.2.** Procedimentos de Teste e Inspeção:

**8.2.1.** Previamente ao recebimento definitivo da solução serão realizados a verificação, testes e inspeção do atendimento integral às especificações técnicas exigidas. Estas ações serão realizadas por equipe designada pelo Diretor do Centro de Processamento de Dados acompanhados dos fiscais do contrato.

**8.2.2.** Inicialmente deverá ser realizada a verificação das especificações exigidas através da inspeção física dos equipamentos, análise dos manuais técnicos enviados juntamente com os equipamentos ou disponibilizados de alguma forma e da análise de informações disponibilizadas no site da fabricante. Para esta etapa deve-se observar a seguinte lista de verificação:

**8.2.2.1.** Verificar se a caixa do equipamento foi entregue lacrada, em embalagem original e apresentando identificações de marca e modelo de acordo a descrição da proposta da CONTRATADA;

**8.2.2.2.** Verificar se o equipamento está novo e sem uso;

**8.2.2.3.** Verificar se o equipamento é o mesmo equipamento que foi ofertado na proposta;

**8.2.2.4.** Verificar se o equipamento foi entregue acompanhado de todos os acessórios previstos nas especificações técnicas (como cabo de energia, conectores, etc.) e descritos na documentação apresentada junto com a proposta da CONTRATADA;

**8.2.2.5.** Verificar se o(s) equipamentos(s) foram entregues na(s) quantidade(s) correta(s);

**8.2.2.6.** Verificar se a documentação mínima exigida foi entregue (exceto relatório de implantação);

**8.2.2.7.** Verificar se os equipamentos foram recebidos de forma que funcionem na tensão elétrica 220 V.

**8.2.3.** Após, deverá ser conduzida a inspeção através da verificação da conformidade da execução dos serviços em relação aos requisitos exigidos nas especificações técnicas.

**8.2.4.** Para avaliação, serão considerados relatórios das ferramentas, verificação das configurações, testes de uso das funcionalidades, documentações de projeto, manuais das soluções e quaisquer outros documentos pertinentes. Para esta etapa deve-se observar a seguinte lista de verificação:

**8.2.4.1.** Conectar cabos de alimentação e verificar funcionamento dos equipamentos;

**8.2.4.2.** Conectar cabos UTP e fibra óptica, e verificar funcionamentos das portas dos equipamentos;

**8.2.4.3.** Realizar configurações relacionadas à rede (configuração de interfaces, endereços IP, roteamento, resolução de nomes (DNS);

**8.2.4.4.** Realizar a criação de objetos, de políticas de segurança e regras de firewall;

**8.2.4.5.** Realizar a configuração do serviço DHCP, configurar modo de alta disponibilidade, com um firewall em modo ativo e outro em modo passivo;

**8.2.4.6.** Verificar a sincronização entre equipamentos (firewall ativo e passivo);

**8.2.4.7.** Verificar o funcionamento do modo de alta disponibilidade, através da simulação de falta de conexão no firewall configurado em modo ativo;

**8.2.4.8.** Caso o software de gerenciamento seja entregue em appliance virtual, verificar a compatibilidade com o hypervisor KVM, criar máquina virtual e realizar as configurações necessárias;

**8.2.4.9.** Realizar a configuração de SNMP para integrar os equipamentos a ferramenta utilizada na Universidade para monitoramento de ativos de rede;

**8.2.4.10.** Realizar a configuração do software de gerenciamento centralizado e armazenamento de logs, e verificar a integração e sincronismo entre os o firewall e o software;

**8.2.4.11.** Verificar o armazenamento de logs e a criação de relatórios pré-definidos e customizados;

**8.2.4.12.** Testar as seguintes funcionalidades no firewall:

**8.2.4.12.1.** Detecção de intrusão (Intrusion Prevention System - IPS) de tráfego malicioso;

**8.2.4.12.2.** Decriptografar tráfego SSL para inspeção de conteúdo;

**8.2.4.12.3.** Permitir inspeção em camada 7 (nível de aplicação);

**8.2.4.12.4.** Permitir inspeção de conteúdo com capacidade de identificar e bloquear vulnerabilidades, vírus, malwares conhecidos;

**8.2.4.12.5.** Permitir a distribuição de endereços IPv4 e IPv6 para clientes, através do serviço DHCP;

**8.2.4.12.6.** Realizar a tradução de endereços IP: NAT (Network Address Translation);

**8.2.4.12.7.** Permitir a criação de redes seguras (VPN) de forma simples para que os usuários e os administradores possam utilizar da infraestrutura da Universidade remotamente;

**8.2.4.12.8.** Permitir autenticação centralizada tanto da rede cabeada como da rede sem fio utilizando-se da base LDAP existente;

**8.2.4.12.9.** Permitir que a autenticação da rede sem fio seja integrada (single sign on), utilizando o protocolo RADIUS, com a solução de WIFI existente, marca Cisco, controladora modelo 5508;

**8.2.4.12.10.** Deverá ser analisada a performance da solução na infraestrutura da SEDUC/PI, verificando principalmente possíveis perdas de pacotes durante o uso da solução com todas as funcionalidades de inspeção e IPS/IDS ativas simultaneamente;

**8.2.4.12.11.** Realizar testes de performance, com ênfase no throughput, utilizando ferramentas capazes de gerar relatórios relacionados a largura de banda;

**8.2.4.12.12.** Também deverá ser realizado um método comparativo de verificação entre os requisitos da solução e os prospectos do fabricante.

**8.2.5.** A Metodologia de Avaliação da Qualidade será realizada pela Contratante, de acordo com a avaliação das seguintes condições que deverão ser cumpridas pela Contratada:

**8.2.5.1.** O cumprimento dos prazos e outras obrigações assumidas pela contratada;

**8.2.5.2.** Entrega da documentação exigida;

**8.2.5.3.** Atendimento dos critérios de aceitação;

**8.2.5.4.** Execução dos procedimentos corretos para que haja o recebimento dos bens e a atestação dos serviços prestados no suporte técnico;

**8.2.5.5.** A Metodologia de Avaliação da Qualidade dos serviços prestados ocorrerá através do acompanhamento e avaliação dos atendimentos aos chamados de suporte técnico especializado junto com as solicitações de garantia;

**8.2.5.6.** Durante a vigência do suporte técnico, A fiscalização técnica dos contratos avaliará constantemente a prestação do serviço e usará como indicador a tabela disponível no item 7.3. Níveis Mínimos de Serviço Exigidos;

**8.2.5.7.** A CONTRATANTE reserva-se o direito de efetuar inspeções e diligências para sanar quaisquer dúvidas existentes, podendo efetuá-las de maneira presencial ou através de documentação, em qualquer momento da contratação.

**8.3.** Níveis Mínimos de Serviço Exigidos:

**8.3.1.** Os chamados poderão ser abertos diretamente com a contratada ou autorizada oficial do fabricante no Brasil através de ligação telefônica gratuita (0800) no idioma português, website ou e-mail. O suporte deverá estar disponível na modalidade de 24x7 (24 horas por dia, 7 dias por semana).

**8.3.2.** O suporte deverá respeitar os seguintes tempos de resposta para os níveis de severidade abaixo:

**8.3.2.1.** Crítica: significa que o produto ficou inoperante ou ocorreu falha de grande impacto e o sistema está parado. Para este nível de severidade o atendimento deverá ser imediato e com tempo de resposta de até 1 (uma) hora para resolução total ou encontro de solução temporária de contorno. Neste caso o chamado deverá ser aberto via telefone (0800);

**8.3.2.2.** Alta: impacto moderado no sistema, travamento, ou parada de ambiente parcial. Para este nível de severidade o tempo de resposta deverá ser de até 2 (duas) horas, em horário comercial, para resolução total ou encontro de solução temporária de contorno;

**8.3.2.3.** Média: Redução de performance do equipamento ou aplicação de solução temporária de contorno bem-sucedida. Para este nível de severidade o tempo de resposta deverá ser de até 4 (quatro) horas, em horário comercial, para resolução total ou encontro de solução temporária de contorno;

**8.3.2.4.** Baixa: dúvidas de configuração ou anomalia de baixo impacto. Para este nível de severidade o tempo de resposta deverá ser de até 8 (oito) horas, em horário comercial.

## 9. MATERIAIS A SEREM DISPONIBILIZADOS:

**9.1.** Para a perfeita execução dos serviços, a Contratada deverá disponibilizar os materiais, equipamentos, ferramentas e utensílios necessários, em qualidade e quantidade suficiente para o perfeito cumprimento do objeto, promovendo sua substituição quando for o caso, conforme a sua metodologia de trabalho, e descrições apresentadas neste Termo de Referência.

**9.2.** Os materiais e/ou equipamentos descritos no Termo de Referência deverão, sempre que possível, seguir as diretrizes de sustentabilidade ambiental estabelecidas no art. 4º do Decreto n° 7.746/2012, observando-se: a origem ambientalmente regular dos recursos naturais utilizados

nos bens; o menor impacto sobre os recursos naturais; a maior eficiência na utilização de recursos naturais como água e energia, quando couber; e a maior vida útil e menor custo de manutenção do bem.

**9.3.** Dentre as recomendações voltadas para sustentabilidade ambiental, a presente licitação observará também os seguintes critérios elencados no art. 5º da Instrução Normativa n° 1 de 19 de janeiro de 2010 da Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão:

**9.4.** Que os bens devam ser, preferencialmente, acondicionados em embalagem individual adequada, com o menor volume possível, que utilize materiais recicláveis, de forma a garantir a máxima proteção durante o transporte e o armazenamento;

**9.5.** Quando couber, que os bens não contenham substâncias perigosas em concentração acima da recomendada na diretiva RoHS (Restrictionof CertainHazardousSubstances), tais como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr(VI)), cádmio (Cd), bifenilpolibromados (PBBs), éteres difenil-polibromados (PBDEs).

**9.6.** Caso necessário, poderá ser solicitada a apresentação de certificação emitida por instituição pública oficial ou instituição credenciada, ou qualquer outro meio de prova que ateste que o bem fornecido cumpre com as exigências estabelecidas.

## 10. OBRIGAÇÕES DA CONTRATANTE

**10.1.** Exigir o cumprimento de todas as obrigações assumidas pela Contratada, de acordo com as cláusulas contratuais e os termos de sua proposta;

**10.2.** Exercer o acompanhamento e a fiscalização dos serviços, por servidor especialmente designado, anotando em registro próprio as falhas detectadas, indicando dia, mês e ano, bem como o nome dos empregados eventualmente envolvidos, e encaminhando os apontamentos à autoridade competente para as providências cabíveis;

**10.3.** Notificar a Contratada por escrito da ocorrência de eventuais imperfeições, falhas ou irregularidades constatadas no curso da execução dos serviços, fixando prazo para a sua correção, certificando-se que as soluções por ela propostas sejam as mais adequadas;

**10.4.** Pagar à Contratada o valor resultante da prestação do serviço, no prazo e condições estabelecidas neste Termo de Referência;

**10.5.** Efetuar as retenções tributárias devidas sobre o valor da Nota Fiscal/Fatura da contratada, no que couber, em conformidade com o item 6 do Anexo XI da IN SEGES/MP n. 5/2017.

**10.6.** Não praticar atos de ingerência na administração da Contratada, tais como:

**10.6.1.** exercer o poder de mando sobre os empregados da Contratada, devendo reportar-se somente aos prepostos ou responsáveis por ela indicados, exceto quando o objeto da contratação previr o atendimento direto, tais como nos serviços de recepção e apoio ao usuário;

**10.6.2.** direcionar a contratação de pessoas para trabalhar nas empresas Contratadas;

**10.6.3.** promover ou aceitar o desvio de funções dos trabalhadores da Contratada, mediante a utilização destes em atividades distintas daquelas previstas no objeto da contratação e em relação à função específica para a qual o trabalhador foi contratado; e

**10.6.4.** considerar os trabalhadores da Contratada como colaboradores eventuais do próprio órgão ou entidade responsável pela contratação, especialmente para efeito de concessão de diárias e passagens.

**10.7.** Fornecer por escrito as informações necessárias para o desenvolvimento dos serviços objeto do contrato;

**10.8.** Realizar avaliações periódicas da qualidade dos serviços, após seu recebimento;

**10.9.** Cientificar o órgão de representação judicial da Advocacia-Geral da União para adoção das medidas cabíveis quando do descumprimento das obrigações pela Contratada;

**10.10.** Arquivar, entre outros documentos, projetos, "as built", especificações técnicas, orçamentos, termos de recebimento, contratos e aditamentos, relatórios de inspeções técnicas após o recebimento do serviço e notificações expedidas;

## 11. OBRIGAÇÕES DA CONTRATADA

**11.1.** Executar os serviços conforme especificações deste Termo de Referência e de sua proposta, com a alocação dos empregados necessários ao perfeito cumprimento das cláusulas contratuais, além de fornecer e utilizar os materiais e equipamentos, ferramentas e utensílios necessários, na qualidade e quantidade mínimas especificadas neste Termo de Referência e em sua proposta;

**11.2.** Reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os serviços efetuados em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

**11.3.** Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, bem como por todo e qualquer dano causado à União ou à entidade federal, devendo ressarcir imediatamente a Administração em sua integralidade, ficando a Contratante autorizada a descontar da garantia, caso exigida no edital, ou dos pagamentos devidos à Contratada, o valor correspondente aos danos sofridos;

**11.4.** Utilizar empregados habilitados e com conhecimentos básicos dos serviços a serem executados, em conformidade com as normas e determinações em vigor;

**11.5.** Vedar a utilização, na execução dos serviços, de empregado que seja familiar de agente público ocupante de cargo em comissão ou função de confiança no órgão Contratante, nos termos do artigo 7° do Decreto n° 7.203, de 2010;

**11.6.** Quando não for possível a verificação da regularidade no Sistema de Cadastro de Fornecedores – SICAF, a empresa contratada deverá entregar ao setor responsável pela fiscalização do contrato, até o dia trinta do mês seguinte ao da prestação dos serviços, os seguintes documentos: 1) prova de regularidade relativa à Seguridade Social; 2) certidão conjunta relativa aos tributos federais e à Dívida Ativa da União; 3) certidões que comprovem a regularidade perante a Fazenda Municipal ou Distrital do domicílio ou sede do contratado; 4) Certidão de Regularidade do FGTS – CRF; e 5) Certidão Negativa de Débitos Trabalhistas – CNDT, conforme alínea "c" do item 10.2 do Anexo VIII-B da IN SEGES/MP n. 5/2017;

**11.7.** Responsabilizar-se pelo cumprimento das obrigações previstas em Acordo, Convenção, Dissídio Coletivo de Trabalho ou equivalentes das categorias abrangidas pelo contrato, por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade à Contratante;

**11.8.** Comunicar ao Fiscal do contrato, no prazo de 24 (vinte e quatro) horas, qualquer ocorrência anormal ou acidente que se verifique no local dos serviços.

**11.9.** Prestar todo esclarecimento ou informação solicitada pela Contratante ou por seus prepostos, garantindo-lhes o acesso, a qualquer tempo, ao local dos trabalhos, bem como aos documentos relativos à execução do empreendimento.

**11.10.** Paralisar, por determinação da Contratante, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de pessoas ou bens de terceiros.

**11.11.** Promover a guarda, manutenção e vigilância de materiais, ferramentas, e tudo o que for necessário à execução dos serviços, durante a vigência do contrato.

**11.12.** Promover a organização técnica e administrativa dos serviços, de modo a conduzi-los eficaz e eficientemente, de acordo com os documentos e especificações que integram este Termo de Referência, no prazo determinado.

**11.13.** Conduzir os trabalhos com estrita observância às normas da legislação pertinente, cumprindo as determinações dos Poderes Públicos, mantendo sempre limpo o local dos serviços e nas melhores condições de segurança, higiene e disciplina.

**11.14.** Submeter previamente, por escrito, à Contratante, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações do memorial descritivo.

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

**11.16.** Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

**11.17.** Cumprir, durante todo o período de execução do contrato, a reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social, bem como as regras de acessibilidade previstas na legislação, quando a contratada houver se beneficiado da preferência estabelecida pela Lei nº 13.146, de 2015.

**11.18.** Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato;

**11.19.** Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, tais como os valores providos com o quantitativo de vale transporte, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da licitação, exceto quando ocorrer algum dos eventos arrolados nos incisos do § 1º do art. 57 da Lei nº 8.666, de 1993.

**11.20.** Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança da Contratante;

**11.21.** Prestar os serviços dentro dos parâmetros e rotinas estabelecidos, fornecendo todos os materiais, equipamentos e utensílios em quantidade, qualidade e tecnologia adequadas, com a observância às recomendações aceitas pela boa técnica, normas e legislação;

**11.22.** Assegurar à CONTRATANTE, em conformidade com o previsto no subitem 6.1, “a”e “b”, do Anexo VII – F da Instrução Normativa SEGES/MP nº 5, de 25/05/2017:

**11.22.1.** O direito de propriedade intelectual dos produtos desenvolvidos, inclusive sobre as eventuais adequações e atualizações que vierem a ser realizadas, logo após o recebimento de cada parcela, de forma permanente, permitindo à Contratante distribuir, alterar e utilizar os mesmos sem limitações;

**11.22.2.** Os direitos autorais da solução, do projeto, de suas especificações técnicas, da documentação produzida e congêneres, e de todos os demais produtos gerados na execução do contrato, inclusive aqueles produzidos por terceiros subcontratados, ficando proibida a sua utilização sem que exista autorização expressa da Contratante, sob pena de multa, sem prejuízo das sanções civis e penais cabíveis.

**11.23.** Comprovar, ao longo da vigência contratual, a regularidade fiscal das microempresas e/ou empresas de pequeno porte subcontratadas no decorrer da execução do contrato, quando se tratar da subcontratação prevista no artigo 48, II, da Lei Complementar n. 123, de 2006.

**11.24.** Substituir a empresa subcontratada, no prazo máximo de trinta dias, na hipótese de extinção da subcontratação, mantendo o percentual originalmente subcontratado até a sua execução total, notificando o órgão ou entidade contratante, sob pena de rescisão, sem prejuízo das sanções cabíveis, ou a demonstrar a inviabilidade da substituição, hipótese em que ficará responsável pela execução da parcela originalmente subcontratada.

**11.25.** Responsabilizar-se pela padronização, pela compatibilidade, pelo gerenciamento centralizado e pela qualidade da subcontratação.

**11.26.** Realizar a transição contratual com transferência de conhecimento, tecnologia e técnicas empregadas, sem perda de informações, podendo exigir, inclusive, a capacitação dos técnicos da contratante ou da nova empresa que continuará a execução dos serviços.

## 12. DA SUBCONTRATAÇÃO

**12.1.** Não será admitida a subcontratação do objeto licitatório.

## 13. ALTERAÇÃO SUBJETIVA

**13.1.** É admissível a fusão, cisão ou incorporação da contratada com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da Administração à continuidade do contrato.

## 14. CONTROLE E FISCALIZAÇÃO DA EXECUÇÃO

**14.1.** O acompanhamento e a fiscalização da execução do contrato consistem na verificação da conformidade da prestação dos serviços, dos materiais, técnicas e equipamentos empregados, de forma a assegurar o perfeito cumprimento do ajuste, que serão exercidos por um ou mais representantes da Contratante, especialmente designados, na forma dos arts. 67 e 73 da Lei nº 8.666, de 1993.

**14.2.** O representante da Contratante deverá ter a qualificação necessária para o acompanhamento e controle da execução dos serviços e do contrato.

**14.3.** A verificação da adequação da prestação do serviço deverá ser realizada com base nos critérios previstos neste Termo de Referência.

**14.4.** A fiscalização do contrato, ao verificar que houve subdimensionamento da produtividade pactuada, sem perda da qualidade na execução do serviço, deverá comunicar à autoridade responsável para que esta promova a adequação contratual à produtividade efetivamente realizada, respeitando-se os limites de alteração dos valores contratuais previstos no § 1º do artigo 65 da Lei nº 8.666, de 1993.

**14.5.** A conformidade do material/técnica/equipamento a ser utilizado na execução dos serviços deverá ser verificada juntamente com o documento da Contratada que contenha a relação detalhada dos mesmos, de acordo com o estabelecido neste Termo de Referência, informando as respectivas quantidades e especificações técnicas, tais como: marca, qualidade e forma de uso.

**14.6.** O representante da Contratante deverá promover o registro das ocorrências verificadas, adotando as providências necessárias ao fiel cumprimento das cláusulas contratuais, conforme o disposto nos §§ 1º e 2º do art. 67 da Lei nº 8.666, de 1993.

**14.7.** O descumprimento total ou parcial das obrigações e responsabilidades assumidas pela Contratada ensejará a aplicação de sanções administrativas, previstas neste Termo de Referência e na legislação vigente, podendo culminar em rescisão contratual, conforme disposto nos artigos 77 e 87 da Lei nº 8.666, de 1993.

**14.8.** As atividades de gestão e fiscalização da execução contratual devem ser realizadas de forma preventiva, rotineira e sistemática, podendo ser exercidas por servidores, equipe de fiscalização ou único servidor, desde que, no exercício dessas atribuições, fique assegurada a distinção dessas atividades e, em razão do volume de trabalho, não comprometa o desempenho de todas as ações relacionadas à Gestão do Contrato.

**14.9.** Durante a execução do objeto, o fiscal técnico deverá monitorar constantemente o nível de qualidade dos serviços para evitar a sua degeneração, devendo intervir para requerer à CONTRATADA a correção das faltas, falhas e irregularidades constatadas.

**14.10.** O fiscal técnico deverá apresentar ao preposto da CONTRATADA a avaliação da execução do objeto ou, se for o caso, a avaliação de desempenho e qualidade da prestação dos serviços realizada.

**14.11.** Em hipótese alguma, será admitido que a própria CONTRATADA materialize a avaliação de desempenho e qualidade da prestação dos serviços realizada.

**14.12.** A CONTRATADA poderá apresentar justificativa para a prestação do serviço com menor nível de conformidade, que poderá ser aceita pelo fiscal técnico, desde que comprovada a excepcionalidade da ocorrência, resultante exclusivamente de fatores imprevisíveis e alheios ao controle do prestador.

**14.13.** Na hipótese de comportamento contínuo de desconformidade da prestação do serviço em relação à qualidade exigida, bem como quando esta ultrapassar os níveis mínimos toleráveis previstos nos indicadores, além dos fatores redutores, devem ser aplicadas as sanções à CONTRATADA de acordo com as regras previstas no ato convocatório.

**14.14.** O fiscal técnico poderá realizar avaliação diária, semanal ou mensal, desde que o período escolhido seja suficiente para avaliar ou, se for o caso, aferir o desempenho e qualidade da prestação dos serviços.

**14.15.** A fiscalização da execução dos serviços abrange, ainda, as seguintes rotinas:

**14.15.1.** Avaliar o cumprimento das regras contidas no Acordo de Nível de Serviço, item 7.3 deste termo de referência.

**14.15.2.** Notificar a Contratada na ocorrência de quebra do acordo.

**14.15.3.** Informar a cada faturamento sobre o valor a ser glosado decorrente da quebra do acordo.

**14.16.** As disposições previstas nesta cláusula não excluem o disposto no Anexo VIII da Instrução Normativa SLTI/MP nº 05, de 2017, aplicável no que for pertinente à contratação.

**14.17.** A fiscalização de que trata esta cláusula não exclui nem reduz a responsabilidade da CONTRATADA, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica corresponsabilidade da CONTRATANTE ou de seus agentes, gestores e fiscais, de conformidade com o art. 70 da Lei nº 8.666, de 1993.

## 15.DO RECEBIMENTO E ACEITAÇÃO DO OBJETO

**15.1.** A emissão da Nota Fiscal/Fatura deve ser precedida do recebimento definitivo dos serviços, nos termos abaixo.

**15.2.** No prazo de até **5 dias corridos** do adimplemento da parcela, a CONTRATADA deverá entregar toda a documentação comprobatória do cumprimento da obrigação contratual;

**15.3.** O recebimento provisório será realizado pelo fiscal técnico e setorial ou pela equipe de fiscalização após a entrega da documentação acima, da seguinte forma:

**15.3.1.** A contratante realizará inspeção minuciosa de todos os serviços executados, por meio de profissionais técnicos competentes, acompanhados dos profissionais encarregados pelo serviço, com a finalidade de verificar a adequação dos serviços e constatar e relacionar os arremates, retoques e revisões finais que se fizerem necessários.

**15.3.1.1.** Para efeito de recebimento provisório, ao final de cada período de faturamento, o fiscal técnico do contrato irá apurar o resultado das avaliações da execução do objeto e, se for o caso, a análise do desempenho e qualidade da prestação dos serviços realizados em consonância com os indicadores previstos, que poderá resultar no redimensionamento de valores a serem pagos à contratada, registrando em relatório a ser encaminhado ao gestor do contrato

**15.3.1.2.** A Contratada fica obrigada a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não atestar a última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.

**15.3.1.3.** O recebimento provisório também ficará sujeito, quando cabível, à conclusão de todos os testes de campo e à entrega dos Manuais e Instruções exigíveis.

**15.3.2.** No prazo de até 10 dias corridos a partir do recebimento dos documentos da CONTRATADA, cada fiscal ou a equipe de fiscalização deverá elaborar Relatório Circunstanciado em consonância com suas atribuições, e encaminhá-lo ao gestor do contrato.

**15.3.2.1.** quando a fiscalização for exercida por um único servidor, o relatório circunstanciado deverá conter o registro, a análise e a conclusão acerca das ocorrências na execução do contrato, em relação à fiscalização técnica e administrativa e demais documentos que julgar necessários, devendo encaminhá-los ao gestor do contrato para recebimento definitivo.

**15.3.2.2.** Será considerado como ocorrido o recebimento provisório com a entrega do relatório circunstanciado ou, em havendo mais de um a ser feito, com a entrega do último.

**15.3.2.2.1.** Na hipótese de a verificação a que se refere o parágrafo anterior não ser procedida tempestivamente, reputar-se-á como realizada, consumando-se o recebimento provisório no dia do esgotamento do prazo.

**15.4.** No prazo de até 10 (dez) dias corridos a partir do recebimento provisório dos serviços, o Gestor do Contrato deverá providenciar o recebimento definitivo, ato que concretiza o ateste da execução dos serviços, obedecendo as seguintes diretrizes:

**15.4.1.** Realizar a análise dos relatórios e de toda a documentação apresentada pela fiscalização e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicar as cláusulas contratuais pertinentes, solicitando à CONTRATADA, por escrito, as respectivas correções;

**15.4.2.** Emitir Termo Circunstanciado para efeito de recebimento definitivo dos serviços prestados, com base nos relatórios e documentações apresentadas; e

**15.4.3.** Comunicar a empresa para que emita a Nota Fiscal ou Fatura, com o valor exato dimensionado pela fiscalização.

**15.5.** O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da Contratada pelos prejuízos resultantes da incorreta execução do contrato, ou, em qualquer época, das garantias concedidas e das responsabilidades assumidas em contrato e por força das disposições legais em vigor (Lei n° 10.406, de 2002).

**15.6.** O gestor emitirá termo circunstanciado para efeito de recebimento definitivo dos serviços prestados, com base nos relatórios e documentação apresentados, e comunicará a CONTRATADA para que emita a Nota Fiscal ou Fatura com o valor exato dimensionado pela fiscalização com base no Instrumento de Medição de Resultado (IMR), ou instrumento substituto.

**15.7.** Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser corrigidos/refeitos/substituídos no prazo fixado pelo fiscal do contrato, às custas da Contratada, sem prejuízo da aplicação de penalidades.

## 16.DO PAGAMENTO

**16.1.** O pagamento será efetuado pela Contratante no prazo de **30 (trinta) dias**, contados do recebimento da Nota Fiscal/Fatura.

**16.1.1.** Os pagamentos decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 24 da Lei 8.666, de 1993, deverão ser efetuados no prazo de até 5 (cinco) dias úteis, contados da data da apresentação da Nota Fiscal/Fatura, nos termos do art. 5º, § 3º, da Lei nº 8.666, de 1993.

**16.2.** A emissão da Nota Fiscal/Fatura será precedida do recebimento definitivo do serviço, conforme este Termo de Referência

**16.3.** A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de

acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 29 da Lei nº 8.666, de 1993.

**16.3.1.** Constatando-se, junto ao SICAF, a situação de irregularidade do fornecedor contratado, deverão ser tomadas as providências previstas no do art. 31 da Instrução Normativa nº 3, de 26 de abril de 2018.

**16.4.** O setor competente para proceder o pagamento deve verificar se a Nota Fiscal ou Fatura apresentada expressa os elementos necessários e essenciais do documento, tais como:

**16.4.1.** o prazo de validade;

**16.4.2.** a data da emissão;

**16.4.3.** os dados do contrato e do órgão contratante;

**16.4.4.** o período de prestação dos serviços;

**16.4.5.** o valor a pagar; e

**16.4.6.** eventual destaque do valor de retenções tributárias cabíveis.

**16.5.** Havendo erro na apresentação da Nota Fiscal/Fatura, ou circunstância que impeça a liquidação da despesa, o pagamento ficará sobrestado até que a Contratada providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a Contratante;

**16.6.** Nos termos do item 1, do Anexo VIII-A da Instrução Normativa SEGES/MP nº 05, de 2017, será efetuada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que a Contratada:

**16.6.1.** não produziu os resultados acordados;

**16.6.2.** deixou de executar as atividades contratadas, ou não as executou com a qualidade mínima exigida;

**16.6.3.** deixou de utilizar os materiais e recursos humanos exigidos para a execução do serviço, ou utilizou-os com qualidade ou quantidade inferior à demandada.

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

**16.8.** Antes de cada pagamento à contratada, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital.

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

**16.10.** Previamente à emissão de nota de empenho e a cada pagamento, a Administração deverá realizar 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.

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

**16.12.** Persistindo a irregularidade, a contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à contratada a ampla defesa.

**16.13.** Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a contratada não regularize sua situação junto ao SICAF.

**16.13.1.** Será rescindido o contrato em execução com a contratada inadimplente no SICAF, salvo por motivo de economicidade, segurança nacional ou outro de interesse público

de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade da contratante.

**16.14.** Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável, em especial a prevista no artigo 31 da Lei 8.212, de 1993, nos termos do item 6 do Anexo XI da IN SEGES/MP n. 5/2017, quando couber.

**16.15.** É vedado o pagamento, a qualquer título, por serviços prestados, à empresa privada que tenha em seu quadro societário servidor público da ativa do órgão contratante, com fundamento na Lei de Diretrizes Orçamentárias vigente.

**16.16.** Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido, de alguma forma, para tanto, fica convencionado que a taxa de compensação financeira devida pela Contratante, entre a data do vencimento e o efetivo adimplemento da parcela é calculada mediante a aplicação da seguinte fórmula:

EM = I x N x VP, sendo:

EM = Encargos moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela a ser paga.

I = Índice de compensação financeira = 0,00016438, assim apurado:

I = (TX)

I = (6/100)/365

I = 0,00016438

TX = Percentual da taxa anual = 6%

## 17. REAJUSTE

17.1 Os preços são fixos e irreajustáveis no prazo de um ano contado da data limite para a apresentação das propostas.

17.1.1 Dentro do prazo de vigência do contrato e mediante solicitação da contratada, os preços contratados poderão sofrer reajuste após o interregno de um ano, aplicando-se o índice IGPM exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

17.2 Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

17.3 No caso de atraso ou não divulgação do índice de reajustamento, o CONTRATANTE pagará à CONTRATADA a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo. Fica a CONTRATADA obrigada a apresentar memória de cálculo referente ao reajustamento de preços do valor remanescente, sempre que este ocorrer.

17.4 Nas aferições finais, o índice utilizado para reajuste será, obrigatoriamente, o definitivo.

17.5 Caso o índice estabelecido para reajustamento venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será adotado, em substituição, o que vier a ser determinado pela legislação então em vigor.

17.6 Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

17.7 O reajuste será realizado por apostilamento.

## 18 GARANTIA DA EXECUÇÃO

18.1 O adjudicatário prestará garantia de execução do contrato, nos moldes do art. 56 da Lei nº 8.666, de 1993, com validade durante a execução do contrato e por 90 (noventa) dias após o término da vigência contratual, em valor correspondente a 5% (cinco por cento) do valor total do contrato.

18.2 No prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, a critério do contratante, contados da assinatura do contrato, a contratada deverá apresentar comprovante de prestação de

garantia, podendo optar por caução em dinheiro ou títulos da dívida pública, seguro-garantia ou fiança bancária.

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

18.2.2 O atraso superior a 25 (vinte e cinco) 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 n. 8.666 de 1993.

18.3 A validade da garantia, qualquer que seja a modalidade escolhida, deverá abranger um período de 90 dias após o término da vigência contratual, conforme item 3.1 do Anexo VII-F da IN SEGES/MP nº 5/2017.

18.3.1 prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;

18.3.2 prejuízos diretos causados à Administração decorrentes de culpa ou dolo durante a execução do contrato;

18.3.3 multas moratórias e punitivas aplicadas pela Administração à contratada; e

18.3.4 obrigações trabalhistas e previdenciárias de qualquer natureza e para com o FGTS, não adimplidas pela contratada, quando couber.

18.4 A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados no item anterior, observada a legislação que rege a matéria.

18.5 A garantia em dinheiro deverá ser efetuada em favor da Contratante, em conta específica na Caixa Econômica Federal, com correção monetária.

18.6 Caso a opção seja por utilizar títulos da dívida pública, estes devem ter sido emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil, e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Fazenda.

18.7 No caso de garantia na modalidade de fiança bancária, deverá constar expressa renúncia do fiador aos benefícios do artigo 827 do Código Civil.

18.8 No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser ajustada à nova situação ou renovada, seguindo os mesmos parâmetros utilizados quando da contratação.

18.9 Se o valor da garantia for utilizado total ou parcialmente em pagamento de qualquer obrigação, a Contratada obriga-se a fazer a respectiva reposição no prazo máximo de 30 (trinta) dias úteis, contados da data em que for notificada.

18.10 A Contratante executará a garantia na forma prevista na legislação que rege a matéria.

18.11 Será considerada extinta a garantia:

18.11.1 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 Contratante, mediante termo circunstanciado, de que a Contratada cumpriu todas as cláusulas do contrato;

18.11.2 no prazo de 90 (noventa) dias após o término da vigência do contrato, caso a Administração não comunique a ocorrência de sinistros, quando o prazo será ampliado, nos termos da comunicação, conforme estabelecido na alínea "h2"do item 3.1 do Anexo VII-F da IN SEGES/MP n. 05/2017.

18.12 O garantidor não é parte para figurar em processo administrativo instaurado pela contratante com o objetivo de apurar prejuízos e/ou aplicar sanções à contratada.

18.13 A contratada autoriza a contratante a reter, a qualquer tempo, a garantia, na forma prevista no neste Edital e no Contrato.

## 19 DAS SANÇÕES ADMINISTRATIVAS

19.1 Comete infração administrativa nos termos da Lei nº 10.520, de 2002, a CONTRATADA que:

19.1.1 Inexecutar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;
19.1.2 ensejar o retardamento da execução do objeto;
19.1.3 falhar ou fraudar na execução do contrato;
19.1.4 comportar-se de modo inidôneo; ou
19.1.5 cometer fraude fiscal.

19.2 Pela inexecução total ou parcial do objeto deste contrato, a Administração pode aplicar à CONTRATADA as seguintes sanções:

19.2.1 Advertência por escrito, quando do não cumprimento de quaisquer das obrigações contratuais consideradas faltas leves, assim entendidas aquelas que não acarretam prejuízos significativos para o serviço contratado;

19.2.2 Multa de:

19.2.2.1 0,1% (um décimo por cento) até 0,2% (dois décimos por cento) por dia sobre o valor adjudicado em caso de atraso na execução dos serviços, limitada a incidência a 15 (quinze) dias. Após o décimo quinto dia e a critério da Administração, no caso de execução com atraso, poderá ocorrer a não-aceitação do objeto, de forma a configurar, nessa hipótese, inexecução total da obrigação assumida, sem prejuízo da rescisão unilateral da avença;

19.2.2.2 0,1% (um décimo por cento) até 10% (dez por cento) sobre o valor adjudicado, em caso de atraso na execução do objeto, por período superior ao previsto no subitem acima, ou de inexecução parcial da obrigação assumida;

19.2.2.3 0,1% (um décimo por cento) até 15% (quinze por cento) sobre o valor adjudicado, em caso de inexecução total da obrigação assumida;

19.2.2.4 0,2% a 3,2% por dia sobre o valor mensal do contrato, conforme detalhamento constante das tabelas 1 e 2, abaixo; e

19.2.2.5 0,07% (sete centésimos por cento) do valor do contrato por dia de atraso na apresentação da garantia (seja para reforço ou por ocasião de prorrogação), observado o máximo de 2% (dois por cento). O atraso superior a 25 (vinte e cinco) dias autorizará a Administração CONTRATANTE a promover a rescisão do contrato;

19.2.2.6 as penalidades de multa decorrentes de fatos diversos serão consideradas independentes entre si.

19.2.3 Suspensão de licitar e impedimento de contratar com o órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente, pelo prazo de até dois anos;

19.2.4 Sanção de impedimento de licitar e contratar com órgãos e entidades da União, com o consequente descredenciamento no SICAF pelo prazo de até cinco anos.

19.2.4.1 A Sanção de impedimento de licitar e contratar prevista neste subitem também é aplicável em quaisquer das hipóteses previstas como infração administrativa no subitem 19.1 deste Termo de Referência.

19.2.5 Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a Contratada ressarcir a Contratante pelos prejuízos causados;

19.3 As sanções previstas nos subitens 19.2.1, 19.2.3, 19.2.4 e 19.2.5 poderão ser aplicadas à CONTRATADA juntamente com as de multa, descontando-a dos pagamentos a serem efetuados.

19.4 Para efeito de aplicação de multas, às infrações são atribuídos graus, de acordo com as tabelas 1 e 2:

Tabela 1

| GRAU | CORRESPONDÊNCIA |
|---|---|

| | |
|---|---|
| 1 | 0,2% ao dia sobre o valor mensal do contrato |
| 2 | 0,4% ao dia sobre o valor mensal do contrato |
| 3 | 0,8% ao dia sobre o valor mensal do contrato |
| 4 | 1,6% ao dia sobre o valor mensal do contrato |
| 5 | 3,2% ao dia sobre o valor mensal do contrato |

Tabela 2

| INFRAÇÃO | | |
|---|---|---|
| ITEM | DESCRIÇÃO | GRAU |
| 1 | Permitir situação que crie a possibilidade de causar dano físico, lesão corporal ou conseqüências letais, por ocorrência; | 05 |
| 2 | Suspender ou interromper, salvo motivo de força maior ou caso fortuito, os serviços contratuais por dia e por unidade de atendimento; | 04 |
| 3 | Manter funcionário sem qualificação para executar os serviços contratados, por empregado e por dia; | 03 |
| 4 | Recusar-se a executar serviço determinado pela fiscalização, por serviço e por dia; | 02 |
| 5 | Retirar funcionários ou encarregados do serviço durante o expediente, sem a anuência prévia do CONTRATANTE, por empregado e por dia; | 03 |
| Para os itens a seguir, deixar de: | | |
| 6 | Registrar e controlar, diariamente, a assiduidade e a pontualidade de seu pessoal, por funcionário e por dia; | 01 |
| 7 | Cumprir determinação formal ou instrução complementar do órgão fiscalizador, por ocorrência; | 02 |
| 8 | Substituir empregado que se conduza de modo inconveniente ou não atenda às necessidades do serviço, por funcionário e por dia; | 01 |
| 9 | Cumprir quaisquer dos itens do Edital e seus Anexos não previstos nesta tabela de multas, após reincidência formalmente notificada pelo órgão fiscalizador, por item e por ocorrência; | 03 |
| 10 | Indicar e manter durante a execução do contrato os prepostos previstos no edital/contrato; | 01 |
| 11 | Providenciar treinamento para seus funcionários conforme previsto na relação de obrigações da CONTRATADA | 01 |

19.5 Também ficam sujeitas às penalidades do art. 87, III e IV da Lei nº 8.666, de 1993, as empresas ou profissionais que:

19.5.1 tenham sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no recolhimento de quaisquer tributos;

19.5.2 tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;

19.5.3 demonstrem não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

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

19.7 As multas devidas e/ou prejuízos causados à Contratante serão deduzidos dos valores a serem pagos, ou recolhidos em favor da União, ou deduzidos da garantia, ou ainda, quando for o caso, serão inscritos na Dívida Ativa da União e cobrados judicialmente.

19.7.1 Caso a Contratante determine, a multa deverá ser recolhida no prazo máximo de 30 (trinta) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

19.8 Caso o valor da multa não seja suficiente para cobrir os prejuízos causados pela conduta do licitante, a União ou Entidade poderá cobrar o valor remanescente judicialmente, conforme artigo 419 do Código Civil.

19.9 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.

19.10 Se, durante o processo de aplicação de penalidade, se 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.

19.11 A apuração e o julgamento das demais infrações administrativas não consideradas como ato lesivo à Administração Pública nacional ou estrangeira nos termos da Lei nº 12.846, de 1º de agosto de 2013, seguirão seu rito normal na unidade administrativa.

19.12 O processamento do PAR não interfere no seguimento regular dos processos administrativos específicos para apuração da ocorrência de danos e prejuízos à Administração Pública Federal resultantes de ato lesivo cometido por pessoa jurídica, com ou sem a participação de agente público.

19.13 As penalidades serão obrigatoriamente registradas no SICAF.

## 20 CRITÉRIOS DE SELEÇÃO DO FORNECEDOR.

20.1 As exigências de habilitação jurídica e de regularidade fiscal e trabalhista são as usuais para a generalidade dos objetos, conforme disciplinado no edital.

20.2 Os critérios de qualificação econômica a serem atendidos pelo fornecedor estão previstos no edital.

20.3 Os critérios de qualificação técnica a serem atendidos pelo fornecedor serão:

20.3.1 Por se tratar de serviço que requer de seu executor conhecimentos técnicos especializados em face do grau de complexidade envolvida, o licitante vencedor deverá apresentar atestado(s), declaração(ões) ou certidão(ões) de capacidade técnica, fornecido por pessoa jurídica, de direito público ou privado, que comprove a prestação de suporte e manutenção de solução de firewall NEXT GENERATION da fabricante BlockBit, de forma satisfatória, pertinente e compatível com o objeto deste Termo de Referência;

20.3.2 As empresas deverão comprovar, ainda, a qualificação técnica, por meio de comprovação de aptidão para a prestação dos serviços em características compatíveis com o

objeto desta licitação, ou com o item pertinente, mediante a apresentação de atestados fornecidos por pessoas jurídicas de direito público ou privado;

20.3.3 Entende-se como compatível com objeto desta licitação a prestação de serviço de manutenção e suporte a solução de firewall NEXT GENERATION da fabricante BlockBit, englobando o suporte ao software e ao hardware;

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

20.3.5 Somente serão aceitos atestados expedidos após a conclusão do contrato ou se decorrido, pelo menos, um ano do início de sua execução, exceto se firmado para ser executado em prazo inferior, conforme item 10.8 da IN SEGES/MPDG n. 5, de 2017;

20.3.6 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 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;

20.3.7 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;

20.3.8 A exigência se faz necessária tendo em vista que a solução afeta diretamente a segurança da informação e a disponibilidade de todos os sites, sistemas e aplicações hospedadas no Centro de Dados da SEDUC disponíveis na Internet. Trata-se de um serviço que é extremamente crítico para a SEDUC e não são admissíveis falhas no processo de suporte. A exigência de expertise do licitante vencedor visa minimizar os riscos relacionados a sustentação dos serviços e a expertise em soluções de outros fabricantes não garante a expertise na referida solução, podendo colocar em risco desnecessário a continuidade na prestação do serviço de segurança provido pela solução;

20.3.9 Requisitos de Experiência Profissional:

20.3.9.1 A empresa deverá possuir no mínimo 01 (um) técnico certificado pelo fabricante da solução;

20.3.9.2 A exigência se faz necessária tendo em vista que a solução afeta diretamente a segurança da informação e a disponibilidade de todos os sites, sistemas e aplicações hospedadas no Centro de Dados da SEDUC disponíveis na Internet. Trata-se de um serviço que é extremamente crítico para a SEDUC e não são admissíveis falhas no processo de suporte. A exigência de expertise do licitante vencedor visa minimizar os riscos relacionados a sustentação dos serviços;

20.3.9.3 Na ocasião da assinatura do contrato o licitante vencedor deverá entregar cópias digitalizadas dos certificados;

20.3.10 Requisitos de Segurança da Informação:

20.3.10.1 Manter sigilo de todos os dados ou informações da SEDUC conforme o Termo de Confidencialidade **(ANEXO I)**, obtidas em função da execução do objeto, sujeitando-se às cominações legais, nos termos da Lei 4.595 de 31.12.1964 e da Lei 13.709 de 14.08.2018 e demais leis correlatas.

20.3.10.2 O representante da Contratante deverá comunicar à Contratada por escrito, quanto à Política de Segurança da Informação da Secretaria de Estado da Educação e suas normas complementares, para ciência e para que se responsabilize por todas as providências e deveres estabelecidos.

20.4 Os critérios de aceitabilidade de preços serão aqueles indicados na tabela do item 1.1 do Termo de Referência.

20.5 O critério de julgamento da proposta é o menor preço global por **grupo único**.

20.6 As regras de desempate entre propostas são as discriminadas no edital.

## 21 ESTIMATIVA DE PREÇOS E PREÇOS REFERENCIAIS.

21.1 O custo estimado da contratação é de **R$ 9.573.789,21 (nove milhões, quinhentos e setenta e três mil, setecentos e oitenta e nove reais e vinte e um centavos).**

## 22 DOS RECURSOS ORÇAMENTÁRIOS.

Gestão/Unidade:140102
Fonte: Tesouro Estadual (000025 – Precatórios do FUNDEF).
Programa de Trabalho:12.368.0002.1956
Elemento de Despesa:4.4.90.52
PI:1956

## 23 INÍCIO DA EXECUÇÃO DOS SERVIÇOS

23.1 A execução dos serviços será iniciada 30 dias após a assinatura do contrato.

Teresina (PI), 22 de dezembro de 2020.

SERPRO
Assinado digitalmente por:
RICARDO LUIZ DE OLIVEIRA FERREIRA
Sua autenticidade pode ser confirmada no endereço :
<http://www.serpro.gov.br/assinador-digital>

**Ricardo Luiz de Oliveira Ferreira**

Gerente de Tecnologia da Informação - GTI

ELLEN GERA DE BRITO MOURA:91330700325

Assinado digitalmente por ELLEN GERA DE BRITO MOURA:91330700325
DN: cn=ELLEN GERA DE BRITO MOURA:91330700325, c=BR, o=ICP-Brasil, ou=RFB e-CPF A3, email=ELLENGERA@GMAIL.COM
Data: 2020.12.22 14:15:03 -03'00'

**Ellen Gera de Brito Moura**

Secretário de Estado da Educação do Piauí

## ANEXO II

## MINUTA TERMO DE CONTRATO

**TERMO DE CONTRATO DE PRESTAÇÃO DE SERVIÇOS Nº ...../...., QUE FAZEM ENTRE SI A SEED/PI, POR INTERMÉDIO DO (A) ..... E A EMPRESA .....**

A **SECRETARIA DE ESTADO DA EDUCAÇÃO - SEDUC/PI**, por meio do(a) ....., com sede na Av. Pedro Freitas, S/N, Centro Administrativo, Blocos D e F, CEP 64018-900, na cidade de Teresina, Estado do Piauí inscrito(a) no CNPJ sob o nº ....., neste ato representado(a) pelo(a) ..... (*cargo e nome*), nomeado(a) pelo Decreto nº ....., de ..... de ..... de 20..., publicada no *DOE* de ..... de ..... de ....., portador da matrícula funcional nº ....., doravante denominada CONTRATANTE, e o(a) ..... inscrito(a) no CNPJ/MF sob o nº ....., sediado(a) na ....., em ..... doravante designada CONTRATADA, neste ato representada pelo(a) Sr.(a) ....., portador(a) da Carteira de Identidade nº ....., expedida pela (o) ....., e CPF nº ....., tendo em vista o que consta no Processo nº ..... e em observância às disposições da às disposições Lei nº 8.666, de 21 de junho de 1993, da Lei nº 10.520, de 17 de julho de 2002, da Lei nº 8.248, de 22 de outubro de 1991, do Decreto nº 9.507, de 21 de setembro de 2018, do Decreto nº 7.174, de 12 de maio de 2010, da Instrução Normativa SGD/ME nº 1, de 4 de Abril de 2019 e da Instrução Normativa SEGES/MPDG nº 5, de 26 de maio de 2017 e suas alterações, do Decreto Estadual n. 15.093/2013, resolvem celebrar o presente Termo de Contrato, decorrente do Pregão nº ...../20...., mediante as cláusulas e condições a seguir enunciadas.

**1. CLÁUSULA PRIMEIRA – OBJETO**

1.1. O objeto do presente instrumento é a contratação de serviços de ....., que serão prestados nas condições estabelecidas no Termo de Referência, anexo I do Edital.

1.2. Este Termo de Contrato vincula-se ao Edital do Pregão, identificado no preâmbulo e à proposta vencedora, independentemente de transcrição.

1.3. Objeto da contratação:

| ITEM | PART NUMBER | DESCRIÇÃO | CATMAT CATSERV | QTDE | Valor de Referência em RS | |
|---|---|---|---|---|---|---|
| | | | | | VALOR UNIT. | VALOR TOTAL |
| 1.1 | BBHWUTM023 | Standard Software License - UTM Subscription - APL BB 10 - for 36 months | xxx | 450 | | |
| 1.2 | BBSSR00289 | Suporte 14x6 - Banco de Horas Mensal - 3hrs - for 36 months | xxx | 450 | | |
| **GRUPO 2: RENOVAÇÃO BB 10000** | | | | | | |
| **ITEM** | **PART NUMBER** | **DESCRIÇÃO** | **CATMAT CATSERV** | **QTDE** | **VALOR UNIT.** | **VALOR TOTAL** |
| 2.1 | BBHWUTM054 | Standard Software License - UTM Subscription Advanced - APL BB 10000 - for 36 months | xxx | 02 | | |
| 2.2 | BBSSR00289 | Suporte 14x6 - Banco de Horas Mensal - 3hrs - for 36 months | xxx | 02 | | |
| **GRUPO 3: AQUISIÇÃO BB 10** | | | | | | |
| **ITEM** | **PART NUMBER** | **DESCRIÇÃO** | **CATMAT CATSERV** | **QTDE** | **VALOR UNIT.** | **VALOR TOTAL** |
| 3.1 | BBHWUTM019 | Hardware Appliance APL UTM BB 10 | xxx | 205 | | |
| 3.2 | BBHWUTM020 | Standard Software License - APL UTM BB 10 | xxx | 205 | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 3.3 | BBHWUTM023 | Standard Software License - UTM Subscription - APL BB 10 - for 36 months | xxx | 205 | | |
| 3.4 | BBSSR00289 | Suporte 14x6 - Banco de Horas Mensal - 3hrs - for 36 months | xxx | 205 | | |
| 3.5 | Instalação – 8 horas | Xxx | xxx | 205 | | |
| **GRUPO 4: AQUISIÇÃO BB 10 SPARE** | | | | | | |
| **ITEM** | **PART NUMBER** | **DESCRIÇÃO** | **CATMAT CATSERV** | **QTDE** | **VALOR UNIT.** | **VALOR TOTAL** |
| 4.1 | BBHWUTM024 | Hardware Appliance APL UTM BB 10 - Spare | xxx | 35 | | |
| 4.2 | BBHWUTM251 | Sistema Operacional Spare - APL UTM BB 10 | xxx | 35 | | |
| **GRUPO 5: AQUISIÇÃO BB 50** | | | | | | |
| **ITEM** | **PART NUMBER** | **DESCRIÇÃO** | **CATMAT CATSERV** | **QTDE** | **VALOR UNIT.** | **VALOR TOTAL** |
| 5.1 | BBHWUTM055 | Hardware Appliance APL UTM BB 50 | xxx | 21 | | |
| 5.2 | BBHWUTM056 | Standard Software License - APL UTM BB 50 | xxx | 21 | | |
| 5.3 | BBHWUTM059 | Standard Software License - UTM Subscription - APL BB 50 - for 36 months | xxx | 21 | | |
| 5.4 | BBSSR00289 | Suporte 14x6 - Banco de Horas Mensal - 3hrs - for 36 months | xxx | 21 | | |
| 5.5 | Instalação – 8 horas | Xxx | xxx | 21 | | |
| | | | | | | **R$** |

| | |
|---|---|
| **VALOR GLOBAL** | **R$ xxxxxx** |

## 2. CLÁUSULA SEGUNDA – VIGÊNCIA

2.1 O prazo de vigência deste Termo de Contrato é aquele fixado no Edital, com início na data de ...../...../..... e encerramento em ...../...../.....

2.1.1 A vigência poderá ultrapassar o exercício financeiro, desde que as despesas referentes à contratação sejam integralmente empenhadas até 31 de dezembro, para fins de inscrição em restos a pagar, conforme Orientação Normativa AGU n° 39, de 13/12/2011.

2.2. A execução dos serviços será iniciada em até 30 (trinta) dias após a assinatura e publicação do extrato do contrato *(indicar a data ou evento para o início dos serviços)*, cujas etapas observarão o cronograma fixado no Termo de Referência.

2.2.1. As etapas 01 e 02 (um e dois) deverão serem executadas após a assinatura do contrato com prazo máximo de 60 (sessenta) dias corridos:

2.2.1.1. Etapas 01 e 02:

2.2.1.2. Renovação de licenças

2.2.2. As etapas 03 (três) a 05 (cinco) especificadas abaixo deverão ser executadas após o recebimento, instalação e a aprovação, por parte da CONTRATANTE, da solução, conforme cronograma elaborado pela CONTRATADA, o qual deve definir um período máximo de execução dessas etapas de 180 (cem e oitenta) dias corridos:

2.2.1. Etapa 03: AQUISIÇÃO BB 10;

2.2.1. Etapa 04: AQUISIÇÃO BB 10 SPARE;

2.2.1. Etapa 05: AQUISIÇÃO BB 50;

2.2.3. Para as Etapas 03 a 05: deverá ser realizada a emissão do Termo de Entrega Definitiva.

2.2.4. As etapas serão consideradas concluídas após a conferência do material e/ou do serviço entregue pela CONTRATADA à CONTRATANTE.

2.2.5. Caso o serviço e/ou material entregue esteja de acordo com este Termo de Referência, a CONTRATANTE emitirá o Termo de Aceite (anexo VI) à CONTRATADA e o pagamento da respectiva etapa será EFETUADO.

2.2.6. O prazo de execução deste contrato é de ....., contados a partir do marco supra referido.

2.3. A CONTRATADA não tem direito subjetivo à prorrogação contratual.

## 3. CLÁUSULA TERCEIRA – PREÇO

3.1. O valor total da contratação é de R$..... (.....)

3.2. No valor acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

3.3 O valor acima é meramente estimativo, de forma que os pagamentos devidos à CONTRATADA dependerão dos quantitativos de serviços efetivamente prestados

## 4. CLÁUSULA QUARTA – DOTAÇÃO ORÇAMENTÁRIA

4.1. As despesas decorrentes desta contratação estão programadas em dotação

orçamentária própria, prevista no orçamento da SEED/PI, para o exercício de 20...., na classificação abaixo:

Gestão/Unidade: 140102

Fonte: Tesouro Estadual (000025 - Precatórios do FUNDEF).

Programa de Trabalho:12368021956

Elemento de Despesa: 3.3.90.39/4.4.90.52

PI: 1956

4.2. No(s) exercício(s) seguinte(s), as despesas correspondentes correrão à conta dos recursos próprios para atender às despesas da mesma natureza, cuja alocação será feita no início de cada exercício financeiro.

**5. CLÁUSULA QUINTA – PAGAMENTO**

5.1. O pagamento será efetuado, de acordo com as etapas do item 5.3 e subitens do Termo de Referência, OBEDECENDO O SEGUINTE CRONOGRAMA, com relação ao valor total do contrato:

| **ITEM 1: RENOVAÇÃO BB 10** | | |
|---|---|---|
| **ITEM** | **DESCRIÇÃO** | **PRAZO DE EXECUÇÃO** |
| 1.1 | Standard Software License - UTM Subscription - APL BB 10 - for 36 months | MÊS 01 |
| 1.2 | Suporte 14x6 - Banco de Horas Mensal - 3hrs - | 36 MESES (CORRESPONDE A |
| **ITEM 2: RENOVAÇÃO BB 10000** | | |
| **ITEM** | **DESCRIÇÃO** | **PRAZO DE EXECUÇÃO** |
| 2.1 | Standard Software License - UTM Subscription Advanced - APL BB 10000 - for 36 months | MÊS 02 |
| 2.2 | Suporte 14x6 - Banco de Horas Mensal - 3hrs - for 36 months | 36 MESES (CORRESPONDE A TODA VIGÊNCIA CONTRATUAL) |
| **ITEM 3: AQUISIÇÃO BB 10** | | |
| **ITEM** | **DESCRIÇÃO** | **PRAZO DE EXECUÇÃO** |
| 3.1 | Hardware Appliance APL UTM BB 10 | MÊS 03 |
| 3.2 | Standard Software License - APL UTM BB 10 | |
| 3.3 | Standard Software License - UTM Subscription - APL BB 10 - for 36 months | |
| 3.4 | Suporte 14x6 - Banco de Horas Mensal - 3hrs - for 36 months | 36 MESES (CORRESPONDE A TODA VIGÊNCIA CONTRATUAL) |
| 3.5 | Serviço de instalação | MÊS 03 E 04 |
| **ITEM 4: AQUISIÇÃO BB 10 SPARE** | | |
| **ITEM** | **DESCRIÇÃO** | **PRAZO DE EXECUÇÃO** |

| | | |
|---|---|---|
| 4.1 | Hardware Appliance APL UTM BB 10 - Spare | MÊS 05 |
| 4.2 | Sistema Operacional Spare - APL UTM BB 10 | |
| **ITEM 5: AQUISIÇÃO BB 50** | | |
| **ITEM** | **DESCRIÇÃO** | **PRAZO DE EXECUÇÃO** |
| 5.1 | Hardware Appliance APL UTM BB 50 | MÊS 06 |
| 5.2 | Standard Software License - APL UTM BB 50 | |
| 5.3 | Standard Software License - UTM Subscription - APL BB 50 - for 36 months | |
| 5.4 | Suporte 14x6 - Banco de Horas Mensal - 3hrs - for 36 months | 36 MESES (CORRESPONDE A TODA VIGÊNCIA CONTRATUAL) |
| 5.5 | Serviço de instalação | MÊS 06 E 07 |

5.1.1. As etapas serão consideradas concluídas após a conferência do material e/ou do serviço entregue pela CONTRATADA à CONTRATANTE.

5.2. O prazo para pagamento à CONTRATADA e demais condições a ele referentes encontram-se definidos no item 16 do Termo de Referência e no Anexo XI da IN SEGES/MPDG n. 5/2017.

**6. CLÁUSULA SEXTA – REAJUSTAMENTO DE PREÇOS EM SENTIDO AMPLO.**

6.1. As regras acerca do reajustamento de preços em sentido amplo do valor contratual (reajuste em sentido estrito e/ou repactuação) são as estabelecidas no item 17.1 do Termo de Referência, anexo a este Contrato.

**7. CLÁUSULA SÉTIMA – GARANTIA DE EXECUÇÃO**

7.1. Será exigida a prestação de garantia na presente contratação, conforme regras constantes do item 18 do Termo de Referência.

**7. CLÁUSULA OITAVA – MODELO DE EXECUÇÃO DOS SERVIÇOS E FISCALIZAÇÃO**

7.1. O modelo de execução dos serviços a serem executados pela CONTRATADA, os materiais que serão empregados, a disciplina do recebimento do objeto e a fiscalização pela CONTRATANTE são aqueles previstos nos itens 8, 14, 15 e 23 do Termo de Referência, anexo I do Edital.

**8. CLÁUSULA NONA – OBRIGAÇÕES DA CONTRATANTE E DA CONTRATADA**

8.1. As obrigações da CONTRATANTE e da CONTRATADA são aquelas previstas nos itens 10 e 11 do Termo de Referência, anexo do Edital.

**9. CLÁUSULA DÉCIMA – SANÇÕES ADMINISTRATIVAS.**

9.1. As sanções relacionadas à execução do contrato são aquelas previstas no item 19 do Termo de Referência, anexo do Edital.

**10. CLÁUSULA DÉCIMA PRIMEIRA – RESCISÃO**

10.1. O presente Termo de Contrato poderá ser rescindido:

10.1.1. por ato unilateral e escrito da Administração, nas situações previstas nos incisos I a XII e XVII do art. 78 da Lei nº 8.666, de 1993, e com as consequências indicadas no art. 80 da mesma Lei, sem prejuízo da aplicação das sanções previstas no Termo de Referência, anexo ao Edital;

10.1.2. amigavelmente, nos termos do art. 79, inciso II, da Lei nº 8.666, de 1993.

10.2. Os casos de rescisão contratual serão formalmente motivados, assegurando-se à CONTRATADA o direito à prévia e ampla defesa.

10.3. A CONTRATADA reconhece os direitos da CONTRATANTE em caso de rescisão administrativa prevista no art. 77 da Lei nº 8.666, de 1993.

10.4. O termo de rescisão, sempre que possível, será precedido de Relatório indicativo dos seguintes aspectos, conforme o caso:

10.4.1. Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

10.4.2. Relação dos pagamentos já efetuados e ainda devidos;

10.4.3. Indenizações e multas.

## 11. CLÁUSULA DÉCIMA SEGUNDA – VEDAÇÕES E PERMISSÕES

11.1. É vedado à CONTRATADA interromper a execução dos serviços sob alegação de inadimplemento por parte da CONTRATANTE, salvo nos casos previstos em lei.

11.2. É permitido à CONTRATADA caucionar ou utilizar este Termo de Contrato para qualquer operação financeira, nos termos e de acordo com os procedimentos previstos na Instrução Normativa SEGES/ME nº 53, de 8 de julho de 2020.

11.2.1. A cessão de crédito, a ser feita mediante celebração de termo aditivo, dependerá de comprovação da regularidade fiscal e trabalhista da cessionária, bem como da certificação de que a cessionária não se encontra impedida de licitar e contratar com o Poder Público, conforme a legislação em vigor, nos termos do Parecer JL-01, de 18 de maio de 2020.

11.2.2. A crédito a ser pago à cessionária é exatamente aquele que seria destinado a cedente (contratada) pela execução do objeto contratual, com o desconto de eventuais multas, glosas e prejuízos causados à Administração, sem prejuízo da utilização de institutos tais como os da conta vinculada e do pagamento direto previstos na IN SEGES/ME nº 5, de 2017, caso aplicáveis.

## 12. CLÁUSULA DÉCIMA TERCEIRA – ALTERAÇÕES

12.1. Eventuais alterações contratuais reger-se-ão pela disciplina do art. 65 da Lei nº 8.666, de 1993, bem como do ANEXO X da IN/SEGES/MPDG nº 05, de 2017.

12.2. A CONTRATADA é obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

12.3. As supressões resultantes de acordo celebrado entre as partes contratantes poderão exceder o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

## 13. CLÁUSULA DÉCIMA QUARTA – DOS CASOS OMISSOS

13.1. Os casos omissos serão decididos pela CONTRATANTE, segundo as disposições contidas na Lei nº 8.666, de 1993, na Lei nº 10.520, de 2002 e demais normas federais aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078, de 1990 – Código de Defesa do Consumidor – e normas e

princípios gerais dos contratos.

## 14. CLÁUSULA DÉCIMA QUINTA – PUBLICAÇÃO

14.1. Incumbirá à CONTRATANTE providenciar a publicação deste instrumento, por extrato, no Diário Oficial do Estado do Piauí – DOE/PI, no prazo previsto na Lei nº 8.666, de 1993.

## 15. CLÁUSULA DÉCIMA SEXTA – FORO

15.1. É eleito o Foro da Seção Judiciária de Teresina - Justiça Estadual, para dirimir os litígios que decorrerem da execução deste Termo de Contrato que não possam ser compostos pela conciliação, conforme art. 55, §2º da Lei nº 8.666/93.

Para firmeza e validade do pactuado, o presente Termo de Contrato foi lavrado em duas (duas) vias de igual teor, que, depois de lido e achado em ordem, vai assinado pelos contraentes e por duas testemunhas.

....., ..... de..... de 20.....

_____

Representante legal da CONTRATANTE

_____

Representante legal da CONTRATADA

Documento assinado eletronicamente por **LEOVIDIO BEZERRA LIMA NETO - Matr.0171745-6**, **Gerente**, em 28/12/2020, às 23:55, conforme horário oficial de Brasília, com fundamento no Cap. III, Art. 14 do Decreto Estadual nº 18.142, de 28 de fevereiro de 2019.

A autenticidade deste documento pode ser conferida no site https://sei.pi.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1008073** e o código CRC **DF179A89**.

## ANEXO III - MODELO DE PROPOSTA DE PREÇO:

Prezados Senhores,

Apresentamos a V.S.ª, nossa proposta de preços de fornecimento dos seguintes equipamentos e serviços, conforme abaixo relacionados.

| ITEM | PART NUMBER | DESCRIÇÃO | CATMAT CATSERV | QTDE | VALOR UNIT. | VALOR TOTAL |
|---|---|---|---|---|---|---|
| 1.1 | BBHWUTM023 | Standard Software License - UTM Subscription - APL BB 10 - for 36 months | xxx | 450 | | |
| 1.2 | BBSSR00289 | Suporte 14x6 - Banco de Horas Mensal - 3hrs - for 36 months | xxx | 450 | | |
| **GRUPO 2: RENOVAÇÃO BB 10000** | | | | | | |
| **ITEM** | **PART NUMBER** | **DESCRIÇÃO** | **CATMAT CATSERV** | **QTDE** | **VALOR UNIT.** | **VALOR TOTAL** |
| 2.1 | BBHWUTM054 | Standard Software License - UTM Subscription Advanced - APL BB 10000 - for 36 months | xxx | 02 | | |
| 2.2 | BBSSR00289 | Suporte 14x6 - Banco de Horas Mensal - 3hrs - for 36 months | xxx | 02 | | |
| **GRUPO 3: AQUISIÇÃO BB 10** | | | | | | |

| ITEM | PART NUMBER | DESCRIÇÃO | CATMAT CATSERV | QTDE | VALOR UNIT. | VALOR TOTAL |
|---|---|---|---|---|---|---|
| 3.1 | BBHWUTM019 | Hardware Appliance APL UTM BB 10 | xxx | 205 | | |
| 3.2 | BBHWUTM020 | Standard Software License - APL UTM BB 10 | xxx | 205 | | |
| 3.3 | BBHWUTM023 | Standard Software License - UTM Subscription - APL BB 10 - for 36 months | xxx | 205 | | |
| 3.4 | BBSSR00289 | Suporte 14x6 - Banco de Horas Mensal - 3hrs - for 36 months | xxx | 205 | | |
| 3.5 | Instalação – 8 horas | Xxx | xxx | 205 | | |
| **GRUPO 4: AQUISIÇÃO BB 10 SPARE** | | | | | | |
| **ITEM** | **PART NUMBER** | **DESCRIÇÃO** | **CATMAT CATSERV** | **QTDE** | **VALOR UNIT.** | **VALOR TOTAL** |
| 4.1 | BBHWUTM024 | Hardware Appliance APL UTM BB 10 - Spare | xxx | 35 | | |
| 4.2 | BBHWUTM251 | Sistema Operacional Spare - APL UTM BB 10 | xxx | 35 | | |
| **GRUPO 5: AQUISIÇÃO BB 50** | | | | | | |
| **ITEM** | **PART NUMBER** | **DESCRIÇÃO** | **CATMAT CATSERV** | **QTDE** | **VALOR UNIT.** | **VALOR TOTAL** |
| 5.1 | BBHWUTM055 | Hardware Appliance APL UTM BB 50 | xxx | 21 | | |
| 5.2 | BBHWUTM056 | Standard Software License - APL UTM BB 50 | xxx | 21 | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 5.3 | BBHWUTM059 | Standard Software License - UTM Subscription - APL BB 50 - for 36 months | xxx | 21 | | |
| 5.4 | BBSSR00289 | Suporte 14x6 - Banco de Horas Mensal - 3hrs - for 36 months | xxx | 21 | | |
| 5.5 | Instalação – 8 horas | Xxx | xxx | 21 | | |
| **VALOR GLOBAL** | | | | | | **R$ xxxxxx** |

O prazo de validade da proposta de preços é de 90 (noventa) dias consecutivos, contados da data da abertura da licitação.

Declaramos que o(s) equipamentos e serviços entregues serão realizados estritamente de acordo com as especificações, condições, exigências constantes do Termo de Referência, bem como, nos seus demais anexos, sob pena de não serem aceitos pelo órgão licitante.

Declaramos que estamos de pleno acordo com todas as condições e exigências estabelecidas no Edital e seus Anexos, bem como aceitamos todas as obrigações e responsabilidades especificadas no edital, termo de referência e contrato.

Declaramos estar cientes da responsabilidade administrativa, civil e penal, bem como ter tomado conhecimento de todas as informações e condições necessárias à correta cotação do objeto licitado.

Declaramos que nos preços propostos estão incluídos todos os custos e despesas, inclusive taxas, impostos, tributos, contribuições sociais, fiscais, comerciais e outros inerentes ao objeto relativo ao procedimento licitatório nº. _____.

Caso nos seja adjudicado o objeto da licitação, nos comprometemos a assinar o contrato no prazo determinado no documento de convocação e, para esse fim, fornecemos os seguintes dados:

Dados da Empresa

Razão Social: _____

CNPJ/MF: _____

Endereço: _____

Tel./Fax: _____

Endereço Eletrônico (e-mail):_____

CEP: _____

Cidade: _____ UF: _____

Banco: ___ Agência: _____ C/C: _____

Dados do Representante Legal da Empresa

Nome:_____

Endereço:_____

CEP: _____ Cidade: _____ UF: _____

CPF/MF: _____ Cargo/Função:_____

RG nº: _____ Expedido por: _____

Naturalidade: _____ Nacionalidade: _____

**OBSERVAÇÕES:**

Havendo discordância entre as especificações deste objeto descritas no COMPRASNET e as especificações constantes do Termo de Referência, prevalecerão as últimas.


Documento assinado eletronicamente por **LEOVIDIO BEZERRA LIMA NETO - Matr.0171745-6**, **Gerente**, em 28/12/2020, às 23:55, conforme horário oficial de Brasília, com fundamento no Cap. III, Art. 14 do Decreto Estadual nº 18.142, de 28 de fevereiro de 2019.

A autenticidade deste documento pode ser conferida no site https://sei.pi.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1008176** e o código CRC **BFD35C09**.

# ANEXO IV

## MODELO DE ATESTADOS E DECLARAÇÕES

### INSTRUÇÕES GERAIS:

As declarações deverão ser emitidas em papel timbrado do Licitante, devendo conter o nome, cargo/função, CPF e o telefone e e-mail de contato do(s) seu(s) representante(s) legal(ais), o(s) qual(is) deverá(ão) constar da indicação a ser apresentada na fase de habilitação, conforme mencionado neste Termo de Referência

Os atestados deverão ser emitidos:

* por empresas privadas brasileiras ou órgãos ou entidades da Administração Pública direta ou indireta; e

* em papel timbrado do Atestante, devendo conter nome e o telefone e e-mail de contato do seu representante, ou qualquer outra forma de que o CLIENTE possa se valer para estabelecer contato;

Os modelos de atestados e declarações foram inseridos no Edital com o objetivo de padronizar as informações apresentadas, facilitar os trabalhos de análise e julgamento pela Comissão de Licitação e evitar que os licitantes sejam inabilitados em razão de falhas ou insuficiência nas informações indicadas. Caso sejam apresentados documentos em formatação diversa, estes deverão contemplar as informações mínimas necessárias à comprovação das exigências para efeitos de habilitação e contratação.

Os atestados e declarações solicitados no Edital, que não tiverem modelo definido neste Anexo, deverão ser elaborados em formato livre seguindo as mesmas instruções gerais acima.

### ANEXO IV.1

### MODELO DE ATESTADO DE EXPERIÊNCIA NA PRESTAÇÃO DE SERVIÇOS REFERENTES AO OBJETO DO EDITAL

Referência: **PREGÃO ELETRONICO Nº ____/202_ - CLIENTE**

Data: _____

Empresa Licitante: _____

CNPJ: _____

ATESTAMOS, para fins de comprovação que a empresa acima referida executou

ou vem executando serviços de_____ similar ou compatível com o objeto deste Termo de Referência.

ATESTAMOS, ainda, que os serviços foram/vêm sendo prestados de forma satisfatória, não havendo em nossos registros nenhum fato que desabone sua conduta e responsabilidade em relação às tarefas assumidas.

_____,_____ de _____ de _____.

Local e data.

Representante da Empresa Atestante:

Nome:_____

Cargo / Função: _____

CPF: _____Telefone: _____

E-mail: _____

OBS.: ESTE ATESTADO DEVERÁ SER EMITIDO EM PAPEL TIMBRADO DA EMPRESA ATESTANTE

**ANEXO IV.2**

**ATESTADO DE VISITA TÉCNICA (VISTORIA)**

Atestado de visita técnica da Licitante às instalações da CONTRATANTE a ser apresentado na habilitação do certame licitatório.

Atestamos, para fins de comprovação junto à Superintendência de Infraestrutura/Comissão de Licitações, relativamente ao Edital de Concorrência Pública nº _____/202_, que o Sr.(a) _____,

CPF_____, representante da empresa _____, Inscrita no CNPJ.: _____ visitou e vistoriou na data abaixo, as instalações físicas do CONTRATANTE – _____, visando obter subsídios para elaboração de sua proposta comercial onde esclareceu todas as dúvidas sobre o objeto da licitação em questão.

_____,_____ de _____ de _____.

Local e Data

_____

Representante da CONTRATANTE

CPF

_____

Representante do LICITANTE

CPF:

**ANEXO IV.3**

**TERMO DE ACEITE DE ATIVIDADE**

| | | |
|---|---|---|
| Logo do Cliente | **TERMO DE ACEITE DE ATIVIDADE** | |
| | | |
| ☐ **Instalação** | ☐ **Treinamento** | ☐ **Corretiva No. Chamado ()** |
| ☐ **Outra:** | | |
| **Descrição da Atividade:** | | |
| **Data** | | |
| **Funcionário CLIENTE** | **Matricula** | **Assinatura** |
| **Funcionário** | **Identificação** | **Assinatura** |
| | | |
| | | |

**ANEXO IV.4**

**TERMO DE RECUSA**

| | | |
|---|---|---|
| Logo do Cliente | **TERMO DE RECUSA DE ATIVIDADE** | |
| | | |
| ☐ **Instalação** | ☐ **Treinamento** | ☐ **Corretiva No. Chamado ( )** |
| ☐ **Outra:** | | |
| **Descrição do motivo da recusa:** | | |

| | | |
|---|---|---|
| **Data** | | |
| **Funcionário CLIENTE** | **Matricula** | **Assinatura** |
| **Funcionário Contratada** | **Identificação** | **Assinatura** |
| | | |

Documento assinado eletronicamente por **LEOVIDIO BEZERRA LIMA NETO - Matr.0171745-6**, **Gerente**, em 28/12/2020, às 23:55, conforme horário oficial de Brasília, com fundamento no Cap. III, Art. 14 do Decreto Estadual nº 18.142, de 28 de fevereiro de 2019.

A autenticidade deste documento pode ser conferida no site https://sei.pi.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1008359** e o código CRC **81DB9B81**.

**Processo SEI: 00011.001163/2020-32** Documento SEI: 1008359

# ANEXO V

## MODELO DE TERMO DE CONFIDENCIALIDADE, ZELO E RESPONSABILIDADE SOBRE OS BENS DE INFORMAÇÃO DA CONTRATANTE

**INSTRUÇÕES GERAIS:**

As declarações deverão ser emitidas em papel timbrado do Licitante, devendo conter o nome, cargo/função, CPF e o telefone e e-mail de contato do(s) seu(s) representante(s) legal(ais), o(s) qual(is) deverá(ão) constar da indicação a ser apresentada na fase de habilitação, conforme mencionado neste Termo de Referência

Os atestados deverão ser emitidos:

* por empresas privadas brasileiras ou órgãos ou entidades da Administração Pública direta ou indireta; e

* em papel timbrado do Atestante, devendo conter nome e o telefone e e-mail de contato do seu representante, ou qualquer outra forma de que o CLIENTE possa se valer para estabelecer contato;

Os modelos de atestados e declarações foram inseridos no Edital com o objetivo de padronizar as informações apresentadas, facilitar os trabalhos de análise e julgamento pela Comissão de Licitação e evitar que os licitantes sejam inabilitados em razão de falhas ou insuficiência nas informações indicadas. Caso sejam apresentados documentos em formatação diversa, estes deverão contemplar as informações mínimas necessárias à comprovação das exigências para efeitos de habilitação e contratação.

Os atestados e declarações solicitados no Edital, que não tiverem modelo definido neste Anexo, deverão ser elaborados em formato livre seguindo as mesmas instruções gerais acima.

**ANEXO V**

**TERMO DE CONFIDENCIALIDADE, ZELO E RESPONSABILIDADE SOBRE OS BENS DE INFORMAÇÃO DA CONTRATANTE**

**CONTRATADO:**

Pelo presente termo de confidencialidade, zelo e responsabilidade, considerando que os bens de informação a mim disponibilizados por força de contrato celebrado com a CONTRATANTE são de propriedade deste e devem ser utilizados com o

único e exclusivo objetivo de permitir a adequada prestação dos serviços contratados e, ciente dos cuidados necessários à preservação e proteção de todos os bens de informação da instituição, inclusive em relação ao dever de sigilo, comprometo-me a:

I – Seguir as diretrizes da política de segurança e proteção dos bens de informação da CONTRATANTE, sob pena de responsabilização penal ou civil cabíveis;

II – Utilizar os bens de informação disponibilizados por força de contrato celebrado com a CONTRATANTE exclusivamente para fins da adequada prestação dos serviços contratados, estritamente em observância aos interesses da CONTRATANTE;

III – Respeitar a propriedade da CONTRATANTE ou de terceiros, sobre os bens de informação disponibilizados, zelando pela integridade dos mesmos, não os corrompendo ou os divulgando a pessoas não autorizadas;

IV – Manter, a qualquer tempo e sob as penas de lei, total e absoluto sigilo sobre os bens de informação da CONTRATANTE, utilizando-os exclusivamente para os fins de interesse deste, estritamente no desempenho das atividades inerentes à prestação dos serviços contratados, não os revelando ou divulgando a terceiros, em hipótese alguma, sem o prévio e expresso consentimento da CONTRATANTE;

V – Instalar e utilizar nos ambientes computacionais disponibilizados pela CONTRATANTE somente softwares desenvolvidos ou adquiridos pela CONTRATANTE;

VI – Permitir a CONTRATANTE a fiscalização, a qualquer tempo, de todos os dados manejados através dos meios fornecidos pela CONTRATANTE em razão da prestação de serviços contratados, pelo que autorizo a CONTRATANTE a monitorar todos os dados manejados nos meios de propriedade do contratante, não configurando o referido monitoramento qualquer quebra de sigilo ou invasão de privacidade;

VII – Não utilizar o ambiente de internet disponibilizado pela CONTRATANTE para uso pessoal, ilícito, ilegal, imoral ou para quaisquer outros fins senão os de estrita prestação dos serviços contratados.

Declaro, ainda, para os devidos fins de direito, que me responsabilizo e obrigo a fazer com que quaisquer de meus agentes, empregados, consultores e demais colaboradores que vierem a ter acesso a quaisquer dados e informações confidenciais cumpram as obrigações constantes deste Termo.

Teresina, ____ de _____ de 202_.

Documento assinado eletronicamente por **LEOVIDIO BEZERRA LIMA NETO - Matr.0171745-6**, **Gerente**, em 28/12/2020, às 23:55, conforme horário oficial de Brasília, com fundamento no Cap. III, Art. 14 do Decreto Estadual nº 18.142, de 28 de fevereiro de 2019.

A autenticidade deste documento pode ser conferida no site https://sei.pi.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1008391** e o código CRC **3448E485**.