ESTADO DA PARAÍBA
ASSEMBLÉIA LEGISLATIVA
COMISSÃO PERMANENTE DE LICITAÇÃO

PREGÃO PRESENCIAL Nº 28/2023

A ASSEMBLEIA LEGISLATIVA DO ESTADO DA PARAIBA, por sua Comissão Permanente de Licitação – CPL, constituída pelo Ato da Mesa Diretora nº 074/2021, publicado no Diário do Poder Legislativo de 01 de dezembro de 2022, torna público, para conhecimento dos interessados, que realizará Licitação na modalidade **PREGÃO PRESENCIAL**, tipo **"MENOR PREÇO POR LOTE¨**, objetivando o fornecimento de serviços para formação de rede de dados através de links IP de Internet terrestres, serviço de segurança e mitigação contra ataques ANTI-DDOS, fornecimento de serviços de segurança de perímetro (controle de Regras de Segurança, Firewall, IPS/IDS, Antivírus, Controle de Conteúdo Web, Controle de Acesso à Aplicações, Emissão de Relatórios Periódicos e Segurança Pró-ativa); Fornecimento de solução SD-WAN, controle de acesso de rede (NAC) e segurança de aplicações WEB e API – WAF, previsto no **Anexo I – Termo de Referência** deste Edital, de acordo com o Processo Administrativo **nº 3244/2023,** que será regido pela Lei Federal nº 10.520/2002, Resolução nº 1.219/2007, subsidiariamente, pela Lei Federal nº 8.666/93 e suas alterações, pela Lei nº 123/2006 e demais legislações pátrias em vigor, consoantes as condições, quantidades e exigências estabelecidas neste Edital e seus Anexos, visando o atendimento das necessidades desta Casa Legislativa.

O recebimento dos Envelopes de Documentação e Propostas de Preços, ocorrerá no dia **29/11/2023 às 09h (nove horas)**, na Sala de Reuniões da Secretaria de Administração e Recursos Humanos, localizada à **Praça Vidal de Negreiros, nº 276 - 3º andar - Sala 327 - Centro, João Pessoa/PB**.

1 – DO OBJETO

O objeto da licitação consiste na contratação de pessoa jurídica para o fornecimento de serviços para formação de rede de dados através de links IP de Internet terrestres, serviço de segurança e mitigação contra ataques ANTI-DDOS, fornecimento de serviços de segurança de perímetro (controle de Regras de Segurança, Firewall, IPS/IDS, Antivírus, Controle de Conteúdo Web, Controle de Acesso à Aplicações, Emissão de Relatórios Periódicos e Segurança Pró-ativa); Fornecimento de solução SD-WAN, controle de acesso de rede (NAC) e segurança de aplicações WEB e API – WAF, para atender as necessidades deste Poder Legislativo, pelo período de 12 (doze) meses, conforme especificações e quantitativos constantes no Anexo I - Termo de Referência deste Edital.

2 – DAS CONDIÇÕES DE PARTICIPAÇÃO

2.1. Poderão participar desta licitação as empresas que atenderem às exigências deste Edital e seus Anexos.

2.1.1. Poderão participar da presente Licitação as pessoas jurídicas do ramo pertinente ao objeto desta licitação, mediante comprovação, nos termos do subitem 3.3.2 deste edital.

2.3. Não será permitida a participação de empresas em consórcio ou que se encontre em Processo de Falência ou Recuperação Judicial ou Extrajudicial, nos termos da Lei nº 11.101/2005 ou que se encontrem incursas nas penalidades previstas no Art. 87, Incisos III e IV (imposta por Órgão da Administração Pública Direta), da Lei nº 8.666/93.

2.4. Não poderá participar da Licitação, direta ou indiretamente, servidor ou dirigente de órgão ou entidade contratante ou responsável pela Licitação.

2.5. É vedado a qualquer participante representar mais de uma empresa licitante, salvo, nos casos de representação para itens distintos.

2.5.1. A empresa proponente somente poderá se pronunciar através de seu representantecredenciado e ficará obrigada pelas declarações e manifestações do mesmo.

3 - DO CREDENCIAMENTO DOS REPRESENTANTES

3.1. Para fins de credenciamento junto ao pregoeiro, a proponente poderá enviar um representante munido de documento que o credencie à participação, respondendo este pela representada; devendo, ainda, no ato de

entrega dos envelopes, identificar-se exibindo a Carteira de Identidade ou outro documento equivalente, com a entrega da respectiva cópia.

3.2. O credenciamento far-se-á mediante a apresentação dos seguintes documentos:

3.2.1. No caso de diretor, sócio ou proprietário da empresa licitante que comparecer ao local, deverá comprovar a representatividade por meio da apresentação de: Ato Constitutivo, Estatuto ou Contrato Social, do documento de eleição de seus administradores, devidamente registrados na Junta Comercial ou no Cartório de pessoas jurídicas, conforme o caso;

3.2.2. Tratando-se de procurador, deverá apresentar Instrumento Público ou Particular de Procuração, com firma reconhecida em Cartório, com poderes expressos para formular ofertas e lances de preços e praticar todos os demais atos pertinentes ao certame, em nome da proponente, acompanhado do correspondente documento, dentre os indicados no subitem acima, que comprove os poderes do mandante para a outorga;

3.2.2.1. O Instrumento de Procuração Público ou Particular deverá estar no prazo de validade nele previstos, e quando não mencionado, será considerada válida dentro do prazo de até 01 (um) ano.

3.3. No momento do credenciamento deverá ser apresentada Declaração de Habilitação, conforme **Anexo III** e de acordo com o Art. 4º, Inciso VII, da Lei Federal nº 10.520/2002 e da Resolução nº 1.219/2007, dando ciência de que cumprem plenamente os requisitos da habilitação.

3.3.1 – EM CASOS DE REPRESENTAÇÃO, O CREDENCIAMENTO FAR-SE-Á ATRAVÉS DE PROCURAÇÃO PÚBLICA OU PARTICULAR, OU, AINDA, CARTA DE CREDENCIAMENTO, CONFORME MODELO APRESENTADO NO ANEXO VIII DO PRESENTE EDITAL, QUE COMPROVE OS NECESSÁRIOS PODERES PARA FORMULAR OFERTAS E LANCES DE PREÇOS, E PRATICAR TODOS OS DEMAIS ATOS PERTINENTES AO CERTAME, EM NOME DA PROPONENTE.

3.3.2 - DEVERÁ SER APRESENTADA CÓPIA AUTENTICADA DO RESPECTIVO ESTATUTO, CONTRATO SOCIAL, OU DOCUMENTO EQUIVALENTE E DA ÚLTIMA ALTERAÇÃO ESTATUTÁRIA OU CONTRATUAL, DEVIDAMENTE REGISTRADO NA JUNTA COMERCIAL, NO QUAL ESTEJAM EXPRESSOS OS PODERES PARA EXERCER DIREITOS E ASSUMIR OBRIGAÇÕES EM DECORRÊNCIA DE TAL INVESTIDURA.

3.3.3 - AS LICITANTES ME E EPP, POR INTERMÉDIO DE SEUS REPRESENTANTES, APRESENTARÃO, AINDA, NA FASE DE CREDENCIAMENTO, DECLARAÇÃO DE QUE NOS TERMOS DA LEICOMPLEMENTAR Nº 123/06, COMPREENDEM-SE COMO SENDO MICROEMPRESAS OU EMPRESAS DE PEQUENO PORTE CONFORME PRESCREVE O ART.3 DA REFERIDA LEI, CONFORME MODELO A SEGUIR:

DECLARAÇÃO

A EMPRESA....., CNPJ N°....., DECLARA SOB AS PENAS DA LEI, QUE PARA PARTICIPAR DO PREGÃO PRESENCIAL Nº ....., ENQUADRA-SE COMO MICROEMPRESA/EMPRESA DE PEQUENO PORTE E QUE SE ENCONTRA DEVIDAMENTE REGISTRADA NO REGISTRO DE EMPRESAS MERCANTIS OU NO REGISTRO CIVIL DE PESSOAS JURÍDICAS (CONFORME O CASO).

LOCAL E DATA

_____
NOME E ASSINATURA DO DIRETOR OU REPRESENTANTE LEGAL

3.4. A declaração falsa relativa ao cumprimento dos requisitos de habilitação, à conformidade da proposta e ao enquadramento como microempresa ou empresa de pequeno porte sujeitará o licitante às sanções previstas neste Edital.

3.5. Será admitido o substabelecimento do credenciamento desde que devidamente justificado e esteja previsto no Instrumento de Procuração e/ou credenciamento poderes específicos para o tal ato.

3.6. A ausência do credenciado a qualquer das fases do certame, será interpretada como desistência da prática dos atos a serem realizados no referido momento.

3.7. Toda a documentação exigida para o certame deverá ser apresentada em cópia legível, devidamente autenticada por Cartório competente **ou por servidor da Administração**, ou publicação em órgão da imprensa oficial, e/ou documento disponível na Internet, no "site" oficial do órgão emissor, sendo que, somente serão considerados válidos aqueles que estejam em plena validade.

3.8. Documentos em fac-símile (FAX) não serão aceitos.

4 - DA ENTREGA DOS ENVELOPES

4.1 - A Comissão Permanente de Licitação - CPL não se responsabilizará por envelopes de "Proposta Comercial" e "Documentação de Habilitação" que não sejam entregues ao Pregoeiro designada, no local, data e horário definidos neste edital.

4.2 - Os envelopes "Proposta Comercial" e "Documentação de Habilitação" deverão ser indevassáveis, hermeticamente fechados e entregues o pregoeiro, na sessão pública de abertura deste certame, conforme endereço, dia e horário especificados abaixo:

ENVELOPE Nº 1 - PROPOSTA DE PREÇOS
À ASSEMBLEIA LEGISLATIVA DO ESTADO DA PARAÍBA
CPL – COMISSÃO PERMANENTE DE LICITAÇÃO
PREGÃO PRESENCIAL Nº 28/2023
DATA/HORA: 29/11/2023 ÀS 09:00h
RAZÃO SOCIAL DO PROPONENTE, ENDEREÇO E CNPJ

ENVELOPE Nº 2 - DOCUMENTOS DE HABILITAÇÃO
À ASSEMBLEIA LEGISLATIVA DO ESTADO DA PARAÍBA
CPL – COMISSÃO PERMANENTE DE LICITAÇÃO
PREGÃO PRESENCIAL Nº 28/2023
DATA/HORA: 29/11/2023 ÀS 09:00h
RAZÃO SOCIAL DO PROPONENTE, ENDEREÇO E CNPJ

5 - DAS PROPOSTAS COMERCIAIS

5.1 - Proposta de Preços deverá ser apresentada em 01 (uma) via, impressa em papel timbrado do licitante, em língua portuguesa, salvo quando às expressões técnicas de uso corrente, redigida com clareza, sem emendas, rasuras, acréscimos ou entrelinhas, devidamente datada, assinada e rubricadas todas as folhas pelo representante legal do licitante proponente, observado o modelo constante do Anexo II deste edital e devendo conter o seguinte:

a) Número do Pregão e o nome ou razão social do proponente, número do CNPJ/MF, endereço completo, telefone, fax e endereço eletrônico (e-mail), este último, se houver, para contato, bem como dados bancários (nome e número do Banco, agência e conta corrente para fins de pagamento).
b) Nome completo do responsável pela assinatura do contrato, profissão, números do CPF e Carteira de Identidade e cargo na empresa.
c) Preço total da proposta, em algarismo e por extenso, em real, com, no máximo, duas casas decimais após a vírgula, prevalecendo este último em caso de divergência, sendo, ainda, considerado preço fixo e irreajustável.
d) Prazo de validade da proposta será de 60 (sessenta) dias consecutivos, a contar da data de sua apresentação.
e) Declaração de que nos preços propostos encontram-se incluídas todas as despesas diretas e indiretas, tributos incidentes, encargos sociais, previdenciários, trabalhistas e comerciais, seguros e demais despesas que incidam sobre a execução dos serviços e quaisquer outros ônus que porventura possam recair sobre o objeto da presente licitação;

5.1.2. Em caso de divergência entre os valores unitários e totais, serão considerados os unitários e, os expressos em algarismos e por extenso, serão considerados os expressos por extenso;

5.1.3. Não será considerada qualquer oferta de vantagem não prevista neste edital;

5.1.4. Aos licitantes interessados fica resguardado o direito de enviar os envelopes de Credenciamento, Proposta Comercial e Documentos de Habilitação por via postal, desde que, sejam **PROTOCOLADOS** na Comissão Permanente de Licitação da Assembléia Legislativa do Estado da Paraíba, localizada na Praça Vidal de Negreiros, nº 276 - 1º andar - sala 125 - Centro, João Pessoa/PB, telefone 3214-4583, com toda a identificação dolicitante e dados pertinentes ao procedimento licitatório em epígrafe e, impreterivelmente, com pelo menos 30 minutos de antecedência ao horário previsto para abertura da sessão pública supracitada.

5.1.4.1. Todo o procedimento de envio e regularidade das informações e conteúdo dos documentos referidos no subitem 5.1.4 corre por conta e risco do licitante.

6 - DA HABILITAÇÃO

Para se habilitarem na presente Licitação, os licitantes deverão apresentar os seguintes documentos, sob pena de inabilitação.

6.1 – Quanto à **regularidade jurídica**:

a) Tratando-se de sociedade comercial, ato constitutivo, estatuto ou contrato social em vigor com todas as suas alterações ou ato constitutivo consolidado, devidamente registrado. No caso de sociedades por ações, tais documentos deverão ser acompanhados da Ata de Eleição de seus Administradores;
b) Tratando-se de sociedades civis, ato constitutivo com todas as suas alterações e sua inscrição, acompanhada de prova da diretoria em exercício;
c) Tratando-se de empresa ou sociedade estrangeira decreto de autorização e ato de registro ou autorização para funcionamento expedido pelo órgão competente, quando a atividade assim o exigir;
d) Tratando-se de empresa individual, o registro comercial;

6.2 – Quanto à **regularidade fiscal e trabalhista**:

a) Prova de inscrição no Cadastro Nacional da Pessoa Jurídica do Ministério da Fazenda (CNPJ).
b) Prova de inscrição no Cadastro de Contribuintes Estadual e/ou Municipal, relativa ao domicílio ou sede da licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual.
c) Prova de regularidade fiscal com a Fazenda Nacional mediante a apresentação de Certidão Negativa de Débitos relativos a Créditos Tributários Federais e à Dívida Ativa da União (CND) ou Certidão Positiva com Efeitos de Negativa de Débitos relativos a Créditos Tributários Federais e à Dívida Ativa da União (CPEND) - (certidão expedida conjuntamente pela RFB e pela PGFN,referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU), inclusive os créditos tributários relativos às contribuições sociais previstas nas alíneas "a", "b" e "c" do parágrafo único do art. 11 da Lei nº 8.212/1991 , às contribuições instituídas a título de substituição, e às contribuições devidas, por lei, a terceiros, inclusive inscritas em DAU).
d) Prova de regularidade perante o Fundo de Garantia do Tempo de Serviço (FGTS) – Certificado de Regularidade para com o FGTS, expedido pela Caixa Econômica Federal.
e) Prova de regularidade com a Fazenda Estadual (Certidão de Tributos Estaduais) emitido pelo órgão competente, da localidade de domicilio ou sede da empresa do proponente, na forma da Lei.
f) Prova de regularidade com a Fazenda Municipal (ISS), emitida pelo órgão competente, da localidade de domicílio ou sede da empresa proponente, na forma da Lei.
g) Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante apresentação da Certidão Negativa de Débitos Trabalhistas – CNDT.

6.3 – Quanto à **qualificação econômico-financeira**:

a) Balanço Patrimonial, devidamente registrado na junta comercial competente, acompanhado das demonstrações contábeis do último exercício financeiro (inclusive o índice de solvência geral) já exigíveis, e apresentados na forma da lei, incluídos os Termos de Abertura e de Encerramento, vedada a sua substituição por balancetes ou

balanços provisórios. São considerados aceitos na forma da lei, o Balanço Patrimonial e as Demonstrações Contábeis que sejam apresentados com assinatura do técnico responsável, devidamente inscrito no Conselho Regional de Contabilidade, e pelo empresário.
b) Certidão Negativa de Falência ou em Processo de Falência ou Recuperação Judicial ou Extrajudicial, nos termos da Lei nº 11.101/2005, expedida pelo Distribuidor do Fórum da sede da pessoa jurídica, observando o prazo estipulado no subitem 10.5 deste Edital.

6.4 – Quanto à **qualificação técnica**:

a) Atestado(s) de Capacidade Técnica da licitante, emitido(s) por entidade da Administração Federal, Estadualou Municipal, direta ou indireta, e/ou empresa privada que comprove, de maneira satisfatória, que a licitante tenha fornecido produtos compatíveis com os do item 03 do Anexo I - Termo de Referência, em papel timbrado do mesmo, constando:

a1) Identificação da empresa, incluindo endereço, telefone e CNPJ;
a2) O(s) atestado(s) deverá(ão) ainda conter o local e a data da sua emissão, bem como a identificação do responsável pela assinatura e seu cargo.
a4) Todo(s) o(s) atestado(s) deverá(ão) ser entregue(s) na versão original ou em cópia autenticada em cartório.

6.4.1 – E, ainda:

a) Declaração, em papel timbrado, com carimbo da empresa e firmado por representante legal desta, de que não emprega menores de 18 anos em trabalho noturno, perigoso ou insalubre, e de que não emprega menores de 16 anos em qualquer trabalho, salvo na condição de aprendiz, a partir de 14 anos, conforme modelo IV;
b) Declaração de Superveniência de fato impeditivo à contratação com a Administração Pública, em papeltimbrado, com carimbo da empresa e firmada por representante legal desta, conforme modelo constante no anexoV;

6.5 - Conforme previsto nos arts. 42 e 43 da LC n° 123/06 (Estatuto Nacional da Microempresa e da Empresa de Pequeno Porte), a comprovação de regularidade fiscal das Microempresas e Empresas de Pequeno Porte somente será exigida para efeito de assinatura do contrato, devendo apresentar toda a documentação exigida para efeito desta comprovação, mesmo que apresente alguma restrição. Havendo alguma restrição referente à comprovação referida, será assegurado o prazo de 05 (cinco) dias úteis, cujo termo inicial corresponderá ao momento em que o proponente for declarado o vencedor do certame, prorrogáveis por igual período, a critério da Administração Pública, para a regularização da documentação, pagamento ou parcelamento do débito, e emissão de eventuais certidões negativas ou positivas com efeito de certidão negativa. A não regularização da documentação, no prazo previsto, implicará decadência do direito à contratação, sem prejuízo das sanções previstas no art. 81 da Lei nº 8.666/93 e nas demais leis referentes à matéria, sendo facultado à Administração convocar os licitantes remanescentes, na ordem de classificação, para a assinatura do contrato, ou revogar a licitação.

6.6 - Todos os documentos apresentados para habilitação deverão estar em nome do licitante, com o número do CNPJ e, preferencialmente, com endereço respectivo, devendo ser observado o seguinte:

a) Se o licitante for a matriz, todos os documentos deverão estar com o número do CNPJ da matriz, ou;
b) Se o licitante for uma filial, todos os documentos deverão estar com o número do CNPJ da filial, exceto quanto à Certidão Negativa de Débito junto ao INSS, por constar no próprio documento que é válido para matriz e filiais, bem assim quanto ao Certificado de Regularidade do FGTS, quando o licitante tenha o recolhimento dos encargos centralizado, devendo, desta forma, apresentar o documento comprobatório de autorização para a centralização, ou;
c) Se o licitante for a matriz e o fornecedor do bem ou prestadora dos serviços for a filial, os documentos deverão ser apresentados com o número de CNPJ da matriz e da filial, simultaneamente;
d) Serão dispensados da apresentação de documentos com o número do CNPJ da filial aqueles documentos que, pela própria natureza, forem emitidos somente em nome da matriz.

6.7 - Os documentos solicitados deverão estar no prazo de validade neles previstos e, quando não mencionado, será considerado válido se dentro do prazo de até 60 (sessenta) dias, contados da data de sua emissão, à

exceção do(s) Atestado(s) de Capacidade Técnica que será(ão) objeto de análise quanto a esse aspecto.

6.8 - **Da substituição da Documentação:** Os documentos exigidos nos subitens **6.1, 6.2 e 6.3. b,** poderão ser substituídos pelo Certificado de Cadastramento e Habilitação - **CECH** em vigor, emitido pelo SIREF – Sistema Integrado de Registro de Fornecedores da **SECRETARIA DE ADMINISTRAÇÃO DO GOVERNO DO ESTADO DA PARAÍBA**.

7 - DA SESSÃO DO PREGÃO

7.1. Após o encerramento do credenciamento e identificação dos representantes das empresas proponentes, o pregoeiro declarará aberta a sessão do Pregão, oportunidade em que não mais aceitará novos proponentes, dando início ao recebimento dos envelopes contendo a Proposta Comercial e os Documentos de Habilitação, exclusivamente dos participantes devidamente credenciados.

8. CLASSIFICAÇÃO DAS PROPOSTAS COMERCIAIS

8.1. Serão selecionadas pelo pregoeiro as propostas de menor preço e as propostas em valores sucessivos e superiores até 10% (dez por cento) à proposta de menor preço, para participarem dos lances verbais.

8.2. Não havendo pelo menos 03 (três) propostas nas condições definidas no item anterior, o Pregoeiro classificará as melhores propostas subsequentes, até o máximo de três, para que seus autores participem dos lances verbais, quaisquer que sejam os preços oferecidos nas propostas apresentadas.

8.3 - LANCES VERBAIS

8.3.1. Aos licitantes classificados será dada oportunidade para nova disputa, por meio de lances verbais e sucessivos, de valores distintos e decrescentes, a partir do autor da proposta classificada de maior preço.

8.3.2. Se duas ou mais propostas em absoluta igualdade de condições ficarem empatadas, como critério de desempate será realizado um sorteio em ato público, para definir a ordem de apresentação dos lances.

8.3.3. A desistência em apresentar lance verbal, quando convocada pelo Pregoeiro, implicará na exclusão do licitante da etapa de lances verbais e na manutenção do último preço apresentado pelo licitante, para efeito de posterior ordenação das propostas.

8.4- JULGAMENTO

8.4.1. O critério de julgamento será o de **MENOR PREÇO POR LOTE**.

8.4.2. Declarada encerrada a etapa competitiva e ordenadas as ofertas, o pregoeiro examinará a aceitabilidade da primeira classificada, quanto ao objeto e valor, decidindo motivadamente a respeito.

8.4.3. Caso não se realizem lances verbais, será verificada a conformidade entre a proposta escrita de menor preço e o valor estimado da contratação.

8.4.4. Em havendo apenas uma oferta e desde que atenda a todos os termos do edital e que seu preço seja compatível com o valor estimado da contratação, esta poderá ser aceita.

8.4.5. Sendo aceitável a oferta de menor preço, será verificado o atendimento das condições de habilitação do licitante que a tiver formulado.

8.4.6. Constatado o atendimento pleno às exigências editalícias, será declarado o proponente vencedor, sendo-lhe adjudicado o objeto para o qual apresentou proposta.

8.4.7. Se a proposta não for aceitável, ou se o proponente não atender às exigências habilitatórias, o pregoeiro examinará as ofertas subseqüentes, verificando a sua aceitabilidade e procedendo à verificação das condições habilitatórias do proponente, na ordem de classificação, até a apuração de uma proposta que atenda ao

edital, sendo o respectivo proponente declarado vencedor e a ele adjudicado o objeto deste edital para o qual apresentou a proposta.

8.4.8. Apurada a melhor proposta que atenda ao edital, o Pregoeiro deverá negociar para que seja obtido um melhor preço.

8.4.9. Não serão aceitos lances verbais com preços simbólicos, irrisórios ou de valor zero.

9. DOS ESCLARECIMENTOS DO RECURSO E IMPUGNAÇÃO DO ATO CONVOCATÓRIO

9.1. Declarada a vencedora, qualquer proponente poderá declinar na própria sessão a intenção motivada de recorrer da decisão.

9.1.1. Admitido o Recurso, o pregoeiro suspenderá a sessão, concedendo o prazo de 03 (três) dias corridos contados da intimação para a apresentação das razões recursais, ficando os demais licitantes desde logointimados para em igual número de dias apresentarem contra razões, que começarão a correr do término do prazo do recorrente, sendo-lhes assegurada vista imediata dos Autos, com a finalidade de subsidiar a preparação dos instrumentos recursais.

9.1.2. O recurso deverá ser dirigido à autoridade superior responsável pela autorização da licitação por intermédio do pregoeiro e deverá declinar sobre a motivação sustentada na sessão.

9.1.3. Acolhidas as razões recursais pelo pregoeiro este retomará a sessão, no dia e hora estabelecida, para a reformulação do ato combatido e consequente adjudicação do objeto ao licitante vencedor.

9.1.4. Não ocorrendo retratação da decisão pelo pregoeiro, este emitirá relatório circunstanciado expondo suas razões de manutenção da decisão e fará subir à autoridade máxima competente para a emissão de parecer final e adjudicação do objeto ao licitante vencedor.

9.1.5. A falta de manifestação imediata e motivada da proponente importará a decadência do direito de recorrer.

9.1.6. Não será concedido prazo para recursos sobre assuntos meramente protelatórios ou quando não justificada a intenção de interpor o recurso pela proponente.

9.1.7. O acolhimento de recurso importará a invalidação apenas dos atos insuscetíveis de aproveitamento.

9.2. Até o 2º (segundo) dia útil anterior à data fixada para recebimento das Propostas e Habilitação, o licitante poderá solicitar esclarecimentos, providências ou impugnar o ato convocatório.

9.2.1. O não exercício de impugnação do prazo acima fixado decairá o direito de fazê-lo administrativamente.

9.2.2. O instrumento de impugnação deverá ser dirigido à autoridade que expediu o ato convocatório.

9.2.3. O acolhimento das razões apresentadas no instrumento de impugnação importará na designação de nova data para a realização da Licitação.

9.2.4. A ausência de decisão administrativa definitiva relativa aos atos combatidos na impugnação em data anterior ao fixado para realização da Licitação, confere ao licitante a sua permanência no certame até a ocorrência deste evento.

9.2.5. Os documentos relativos ao item 9 deste instrumento convocatório poderão ser enviados através do e-mail *cpl.alpb@gmail.com*, nos dias e horários de expediente da Comissão Permanente de Licitação da Assembleia Legislativa da Paraíba, com exceção dos recursos, que deverão ser protocolados no Setor de Protocolo desta Casa Legislativa, nos dias e horários de expediente (segunda-feira, das 13h as 17h; terça-feira a quinta-feira, das 08h as 17h e; sexta-feira, das 08h as 12h).

10 - DA ADJUDICAÇÃO E DA HOMOLOGAÇÃO

10.1. Inexistindo manifestação recursal, o pregoeiro adjudicará o objeto da licitação ao licitante vencedor, com a posterior homologação do resultado pela autoridade competente.

10.2. Decididos os recursos porventura interpostos, e constatada a regularidade dos atos procedimentais, a autoridade competente adjudicará o objeto ao licitante vencedor e homologará o procedimento.

11 - DO CONTRATO

11.1. Encerrado o procedimento licitatório, será elaborado o respectivo Termo de Contrato ou instrumento equivalente, onde o representante legal da proposta vencedora será convocado para firmar o mesmo, desde que obedecidas todas as exigências estabelecidas neste Edital e, de conformidade com a proposta aceita.

11.1.1. O adjudicatário deverá comprovar a manutenção das condições demonstradas para habilitação para assinar o contrato.

11.1.2. Caso o adjudicatário não apresente situação regular no ato da assinatura do contrato, ou recuse-sea assiná-lo, serão convocados os licitantes remanescentes, observada a ordem de classificação, para celebrar o contrato.

11.2. O representante legal da proposta vencedora deverá assinar o contrato ou instrumento equivalente, dentro do prazo máximo de 05 (cinco) dias úteis a contar do recebimento da comunicação para tal, através de fax ou correio eletrônico. Qualquer solicitação de prorrogação de prazo para assinatura do contrato ou instrumento equivalente, decorrente desta licitação, somente será analisada se apresentada antes do decurso do prazo para tal e devidamente fundamentada.

11.3. Qualquer solicitação de prorrogação de prazo para assinatura do contrato ou instrumento equivalente, decorrente desta licitação, somente será analisada se apresentada antes do decurso do prazo para tal e devidamente fundamentada.

12. DAS SANÇÕES ADMINISTRATIVAS

12.1. A recusa do adjudicatário em assinar o Contrato, dentro do prazo estabelecido pela Contratante, bem como o atraso e a inexecução parcial ou total do Contrato, caracterizarão o descumprimento da obrigação assumida e permitirão a aplicação das seguintes sanções pela Contratante:

a) Advertência, que será aplicada sempre por escrito;
b) Multas;
c) Rescisão unilateral do Contrato sujeitando-se a Contratada ao pagamento de indenização à Contratante por perdas e danos;
d) Suspensão temporária do direito de licitar, de participar de licitações e impedimento de contratar com a Administração Pública, por prazo não superior a 2 (dois) anos;
e) Indenização à Contratante da diferença de custo para contratação de outro licitante;
f) Declaração de inidoneidade para licitar e contratar com a Administração Pública.

12.2. A multa será aplicada à razão de 10% (dez por cento) sobre o valor total do material em atraso, por dia de atraso no fornecimento dos materiais.

12.3. O valor máximo das multas não poderá exceder, cumulativamente, a 10% (dez por cento) do valor do contrato.

12.4. As sanções previstas neste Capítulo poderão ser aplicadas cumulativamente, ou não, de acordo com a gravidade da infração, facultada ampla defesa à Contratada, no prazo de 05 (cinco) dias úteis a contar da intimação do ato.

13.2. EXTENSÃO DAS PENALIDADES

13.2.1. A sanção de suspensão de participar em licitação e contratar com a Administração Pública poderá ser aplicada também àqueles que:

a) Retardarem a execução do pregão;
b) Demonstrarem não possuir idoneidade para contratar com a Administração e;
c) Fizerem declaração falsa ou cometerem fraude fiscal.
d) Por atraso injustificado na execução do contrato.

14 - DA ADJUDICAÇÃO E DA HOMOLOGAÇÃO

14.1. Inexistindo manifestação recursal, o pregoeiro adjudicará o objeto da licitação ao licitante vencedor, com a posterior homologação do resultado pela autoridade competente.

14.2. Decididos os recursos porventura interpostos e, constatada a regularidade dos atos procedimentais, a autoridade competente adjudicará o objeto ao licitante vencedor e homologará o procedimento.

15 - DA DOTAÇÃO ORÇAMENTÁRIA

15.1. As despesas decorrentes desta licitação serão custeadas com Recursos Orçamentários da Assembleia Legislativa do Estado da Paraíba, na classificação funcional programática 01101.01122.5046.4216, no elemento de despesa 33903900.100.

16 - DAS DISPOSIÇÕES FINAIS

16.1 Até 02 (dois) dias úteis antes da data fixada para recebimento das propostas, qualquer pessoa poderá solicitar esclarecimentos, providências ou impugnar o ato convocatório do Pregão, quanto a falhas ou irregularidades que o viciarem.

16.2 - Este edital deverá ser lido e interpretado na íntegra, e após apresentação da documentação e da proposta não serão aceitas alegações de desconhecimento ou discordância de seus termos.

16.3 - Será dada vista aos proponentes interessados tanto das Propostas Comerciais como dos Documentos de Habilitação apresentados na sessão.

16.4. Serão desclassificadas as Propostas que se opuserem a quaisquer dispositivos legais vigentes, que consignarem descontos excessivos ou manifestamente inexequíveis, preço global ou unitário simbólicos, irrisórios ou cotação de valor zero.

16.5. É facultada o pregoeiro ou à autoridade superior, em qualquer fase da Licitação, a promoção de diligência destinada a esclarecer ou complementar a instrução do Processo, vedada a inclusão posterior de documento que deveria ser apresentado em sessão pública da Licitação.

16.6. As licitantes são responsáveis pela fidelidade e legitimidades das informações e dos documentos apresentados em qualquer fase da Licitação, bem como, pelo custo da preparação e apresentação dos documentos, independentemente do resultado do processo licitatório.

16.7. 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 e local anteriormente estabelecido, salvo comunicação ao contrário.

16.8. Na contagem dos prazos estabelecidos neste Edital e seus Anexos, excluir-se-á o dia de início e incluir-se-á o do vencimento. Só iniciam e vencem os prazos em dias de expediente na Assembleia Legislativa do Estado da Paraíba – ALPB.

16.9. O descumprimento de exigências formais não essenciais, não importará no afastamento do licitante, desde que seja possível a aferição de sua qualificação e da exata compreensão de sua Proposta, durante a realização da sessão pública da Licitação.

16.10. As normas que disciplinam esta Licitação serão sempre interpretadas em favor da ampliação da disputa entre os interessados, sem o comprometimento dos princípios de que regem o procedimento licitatório e o Contrato.

16.11. A presente licitação somente poderá ser revogada por razões de interesse público, decorrente de fato superveniente devidamente comprovado ou, anulada, no todo ou em parte, por ilegalidade de ofício ou por provocação de terceiros, mediante parecer escrito e devidamente comprovado.

16.12. O ato de homologação do procedimento não confere o direito à contratação.

16.13. Os casos omissos serão resolvidos pelo Pregoeiro com base na legislação vigente.

16.14. Os envelopes contendo a "Documentação e Propostas" eliminadas do certame ficarão a disposição dos licitantes pelo prazo máximo de 15 (quinze) dias úteis do encerramento da Licitação. Após este período, serão destruídos.

16.15. As decisões do pregoeiro serão consideradas definitivas somente após homologação do procedimento pela Mesa Diretora da Assembleia Legislativa da Paraíba.

16.16. O PREGOEIRO, NO INTERESSE DA ADMINISTRAÇÃO, PODERÁ RELEVAR OMISSÕES PURAMENTE FORMAIS OBSERVADAS NA DOCUMENTAÇÃO E PROPOSTA, DESDE QUE NÃO CONTRARIEM A LEGISLAÇÃO VIGENTE E NÃO COMPROMETAM A LISURA DA LICITAÇÃO, SENDO POSSÍVEL A PROMOÇÃO DE DILIGÊNCIA DESTINADA A ESCLARECER OU A COMPLEMENTAR A INSTRUÇÃO DO PROCESSO, PODENDO TAMBÉM ESTABELECER UM PRAZO DE 24 HORAS PARA RESOLUÇÃO DAS DILIGÊNCIAS. O NÃO CUMPRIMENTO DO PRAZO ACARRETARÁ EM AUTOMÁTICA INABILITAÇÃO OU DESCLASSIFICAÇÃO, CONFORME O CASO.

16.17. A critério do pregoeiro a sessão poderá ser suspensa e reiniciada em dia e horário definidos por ele, o qual será registrado em Ata.

16.18. Compete ao pregoeiro suprimir as incorreções meramente formais por meio de **ERRATA** do pregão, devidamente acostada aos autos do processo físico.

16.19. Informações ou esclarecimentos adicionais sobre a presente Licitação poderão ser obtidos junto à Comissão Permanente de Licitação – CPL da Assembleia Legislativa da Paraíba, localizada à Praça Vidal de Negreiros, nº 276 - 1º andar - Sala 125 - Centro, João Pessoa/PB; no link *http://www.al.pb.leg.br/transparencia/administracao/licitacoes*; bem como via e-mail, através do endereço eletrônico cpl.alpb@gmail.com, ou pelo telefone (83) 3214-4583.

16.20. Fica eleito o foro da cidade de João Pessoa - PB, renunciando a qualquer outro, por mais privilegiado que seja, para processar as questões resultantes desta Licitação e que não possam ser dirimidas administrativamente.

16.21. Integram o presente Edital, independentemente de qualquer transcrição: Anexo I (Termo de Referência), Anexo II (Modelo de Proposta de Preços, Anexo III (Declaração de Habilitação), Anexo IV (Declaração de Menor); Anexo V (Declaração de Compromisso); Anexo VI (Carta de credenciamento) e Anexo VII (Minuta de contrato).

João Pessoa, 14 de novembro de 2023.

RENATO CALDAS LINS JUNIOR
Pregoeiro

PREGÃO PRESENCIAL Nº 28/2023

ANEXO I

TERMO DE REFERÊNCIA

1 - DO OBJETO

1.1. O objeto da licitação consiste na **contratação de pessoa jurídica** para o Fornecimento de serviços para formação de rede de dados através de links IP de Internet terrestres, serviço de segurança e mitigação contra ataques ANTI-DDOS, fornecimento de serviços de segurança de perímetro (controle de Regras de Segurança, Firewall, IPS/IDS, Antivírus, Controle de Conteúdo Web, Controle de Acesso à Aplicações, Emissão de Relatórios Periódicos e Segurança Pró-ativa); Fornecimento de solução SD-WAN, controle de acesso de rede (NAC) e segurança de aplicações WEB e API – WAF, para atender as necessidades deste Poder Legislativo, pelo período de 12 (doze) meses, conforme especificações e quantitativos constantes deste Termo de Referência.

2 – JUSTIFICATIVA

2.1. Visando imprimir maior celeridade dos trabalhos, a Assembleia Legislativa do Estado da Paraíba disponibiliza em meio eletrônico, através de seu sítio na Internet, diversas consultas, notícias, documentos e serviços aos cidadãos, servidores e membros.

2.2. Justifica-se a contratação dos Serviços tendo em vista serem eles essenciais ao bom e pleno desempenho das atividades fim da **ASSEMBLEIA LEGISLATIVA DO ESTADO DA PARAÍBA** e unidades interligadas, outro fato é o encerramento do contrato atual, para a prestação dos serviços dos Links de comunicação junto a Empresa fornecedora do atual link e segurança de rede que interliga a Sede da **ALPB, ESCOLA INFANTIL, ESCOLA DO LEGISLATIVO E SEUS ANEXOS** ao serviço de comunicação da rede interna e internet.
.
2.3. Os serviços são de grande importância para os trabalhos desta Casa Legislativa pois além de acesso da Casa a internet fornece IPS para que nossos Serviços (SAPL, ZOOM, Portais, Sites, Transmissões das Sessões e reuniões desta Casa para as redes socias e etc.) estejam disponíveis para toda a população através da internet. Os serviços solicitados também colaboram para adequar a Assembleia Legislativa da Paraíba a LGPD (Lei Geral de Proteção de Dados).

3 - CLASSIFICAÇÃO DOS SERVIÇOS

3.1. Os serviços a serem contratados enquadram-se na classificação de serviços comuns, nos termos da Lei n 10.520/2022 e do Decreto Estadual n 24.649/2003.

4 - CARACTERISTICAS GERAIS DOS SERVIÇOS

4.1. Fazem parte do presente Edital os seguintes serviços, a serem contratados em 02 (dois) lotes:

a) Fornecimento de serviço de acesso IP dedicado à Internet com CPE e serviço mitigação contra-ataques Anti-DDoS;
b) Fornecimento de serviços de solução de segurança de redes NGFW tipos 1 e 2 (controle de Regras de Segurança, Firewall, IPS/IDS, Controle de Conteúdo Web, Controle de Acesso à Aplicações, Emissão de Relatórios Periódicos e Segurança Pró-ativa);
c) Fornecimento de serviços de solução de controle de acesso de rede (NAC);
d) Fornecimento de serviços de solução de segurança de aplicações WEB e API – WAF.

5 - DESCRIÇÃO DOS SERVIÇOS

5.1. Fornecimento de rede de links IP de acesso à Internet com serviço de segurança e mitigação contra-ataques DDoS;

5.1.1.Conexão física e lógica do circuito/porta de acesso até o local determinado pela CONTRATANTE;

5.1.2. O circuito de acesso será disponibilizado na sua totalidade em meio físico terrestre através de Fibra Óptica;

5.1.3. A velocidade de acesso, tanto para o circuito como para a porta do Backbone utilizado pela contratada será conforme lista de endereços no ANEXO II;

5.1.4. Fornecimento de 16 endereços IP's válidos por link/acesso;

5.1.5. A CONTRATADA disponibilizará central de atendimento para comunicação de falhas e inoperâncias do circuito/porta de acesso. O atendimento será prestado através de ligação telefônica gratuita via 0800, disponível 24 horas por dia, sete dias por semana e-mail ou mensagens através de whatsapp corporativo.;

5.1.6. Qualquer interrupção programada pela CONTRATADA será comunicada com pelo menos 7 (sete) dias de antecedência e com aprovação da CONTRATANTE;

5.1.7. O tempo de interrupção não programada não será superior a 6 (seis) horas na capital;

5.1.8. Quanto à disponibilidade do circuito:

5.1.8.1. O índice mínimo de disponibilidade do Backbone IP de uso da CONTRATADA deverá ser de 99,35% conforme as condições abaixo relatadas;

5.8.1.2. Todos os serviços de comunicação de dados estarão disponíveis 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, todos os dias do ano;

5.1.8.3. A disponibilidade do serviço indicará o percentual de tempo, durante o período de 1 (um) mês de operação, em que o circuito integrante do serviço permanecer em condições normais de funcionamento;

5.1.8.4. A condição normal de funcionamento de um circuito significa o perfeito funcionamento de todos os elementos que o compõem, a saber: enlaces físicos, interfaces, roteadores, concentradores, repetidores, recursos alocados na rede da CONTRATADA, etc.

5.1.8.5. O serviço será considerado indisponível a partir do início de uma interrupção registrada na gerência/supervisão da CONTRATADA até o restabelecimento do circuito à condição normal de funcionamento e a respectiva informação a CONTRATANTE;

5.1.8.6. A disponibilidade do serviço será calculada para um período de 1 (um) mês através da seguinte equação:

$D = \frac{T_0 - T_i}{T_0} \times 100$	**Onde:** **D** = disponibilidade; **To** = período de operação (1 mês), em minutos; **Ti** = tempo total de indisponibilidade do circuito de acesso, ocorrida no período de operação (1 mês), em minutos.

5.1.8.7. No cálculo de disponibilidade de um circuito, não serão considerados os períodos de tempo em que o mesmo estiver sendo atendido através de sua solução de contingência;

5.1.8.8. No cálculo de disponibilidade, não serão consideradas as interrupções de responsabilidade da CONTRATANTE, nem as interrupções programadas pela CONTRATADA e aprovadas pela CONTRATANTE.

5.1.9. Índices de desempenho de referência:

5.1.9.1. Latência média mensal entre o BackBone IP (PE) utilizado pela CONTRATADA e o equipamento no ambiente da contratante (CE) menor ou igual a 70ms;

5.1.9.2. Perda de Pacotes Média Mensal do Núcleo do Backbone IP: menor ou a 1%.

5.1.10. A CONTRATADA deverá possuir central de atendimento através de número 0800 (em língua portuguesa) para registro de reclamações, acionamento de reparo, e assistência técnica.

5.1.11. Os serviços de ativação e instalação dos circuitos e equipamentos deverão ser prestados no ambiente computacional da CONTRATANTE;

5.1.12. A CONTRATADA deverá entregar a solução totalmente operacional, com os níveis de serviços exigidos, incluindo equipamentos e circuitos de comunicação, em até 90 (noventa) dias, prorrogáveis por mais 30 dias caso devidamente justificado pela contratada.

5.1.13. Serviço de segurança e mitigação contra ataques DDOS

5.1.13.1. Acesso corporativo exclusivo e dedicado à Internet;

5.1.13.2. A CONTRATADA deverá prover saída de Internet internacional que não utilize outras operadoras brasileiras como trânsito IP.

5.1.13.3. Para proteção do acesso IP, a CONTRATADA deverá disponibilizar proteção contra-ataques de negação de serviço, evitando assim a saturação da banda da Internet e indisponibilidade dos serviços em momentos de ataques DOS (Denial of Service) e Anti-DDoS (Distributed Denial of Service);

5.1.13.4. A solução DDoS deverá prover o serviço de mitigação de ataques de negação de serviço (DoS - Denial of Service) para o circuito de conectividade IP dedicada à Internet, sejam eles distribuídos (Anti-DDoS - Distributed Denial of Service) ou não;

5.1.13.5. A CONTRATADA deve utilizar no mínimo 1 (um) centro de limpeza nacional;

5.1.13..6. Não haverá taxa adicional por volume de mitigação de ataques (Anti-DDoS - Distributed Denial of Service) nos IP's monitorados;

5.1.13.7. A alteração de capacidade de mitigação deverá ser implementada em um prazo máximo de 5 dias úteis, a contar da data de solicitação formal através de correio eletrônico encaminhado via chave oficial ou de autorizados pela contratante;

5.1.13.8. O ataque deve ser mitigado separando o tráfego legítimo do malicioso, de modo que os serviços de Internet providos pelo cliente continuem disponíveis;

5.1.13.9. A limpeza do tráfego deverá ser seletiva e atuar somente sobre os pacotes destinados ao IP atacado, todo tráfego restante não deverá sofrer nenhuma forma de limpeza ou desvio;

5.1.13.10. A solução deve possuir mecanismos para filtragem de pacotes anômalos, garantindo a validade das conexões, sem efetuar qualquer limitação com base no número de sessões ou de pacotes por endereço, de modo a evitar o bloqueio de usuários legítimos;

5.1.13.11. A CONTRATADA deve tomar todas as providências necessárias para recompor a disponibilidade do link em caso de incidentes de ataques de Anti-DDoS, recuperando o pleno funcionamento do mesmo;

5.1.13.12. Para a mitigação dos ataques o tráfego só deverá ser encaminhado para limpeza fora do território brasileiro nos casos em que os centros nacionais não suportarem a capacidade de mitigação e a demanda de ataques os ataques de origem nacional deverão ser tratados nos centros nacionais e os de origem internacional nos centros internacionais

5.1.13.13. A solução deverá possuir funcionalidades de monitoramento, detecção e mitigação de ataques, mantidas em operação ininterrupta durante as 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana, no período de vigência contratual;

5.1.13..14. A análise realizada para fins da solução deverá ser passiva sem utilização de elementos da rede da contratante para coleta dos dados a serem analisados;

5.1.13.15. A mitigação de ataques deve ser baseada em arquitetura na qual há o desvio de tráfego suspeito comandado pelo equipamento de monitoramento, por meio de alterações do plano de roteamento;

5.1.13.16. A solução não poderá desviar o tráfego de ataque para fora do seu ASN;

5.1.13.17. A solução de mitigação de ataques volumétricos na nuvem da operadora deverá atuar com desvio de rotas via BGP para o host que está sendo atacado /24;

5.1.13.18. A solução deve manter uma lista dinâmica de endereços IP bloqueados, retirando dessa lista os endereços que não enviarem mais requisições maliciosas após um período considerado seguro por um determinado cliente;

5.1.13.19. A solução deve suportar a mitigação automática de ataques, utilizando múltiplas técnicas como White Lists, Black Lists, limitação de taxa, técnicas desafio-resposta, descarte de pacotes malformados, técnicas de mitigação de ataques aos protocolos HTTP/HTTPS, DNS, VPN, FTP, NTP, UDP, ICMP, bloqueio por localização geográfica de endereços IP, dentre outras;

5.1.13.20. A solução deve implementar mecanismos capazes de detectar e mitigar todos e quaisquer ataques que façam o uso não autorizado de recursos de rede, para protocolo IPv4 e IPv6, incluindo, mas não se restringindo aos seguintes:

5.1.13.20.1. Ataques de inundação (Bandwidth Flood), incluindo Flood de UDP e ICMP;

5.1.13.20.2. Ataques à pilha TCP, incluindo mal-uso das Flags TCP, ataques de RST e FIN, SYN Flood e TCP Idle Resets;

5.1.13.20.3. Ataques que utilizam Fragmentação de pacotes, incluindo pacotes IP, TCP e UDP;

5.1.13.20.4. Ataques de Botnets, Worms e ataques que utilizam falsificação de endereços IP origem (IP Spoofing);

5.1.13.21. Em nenhum caso será aceito bloqueio de ataques de DOS e ANTI-DDOS por ACLs em roteadores de bordas da contratada;

5.1.13.22. Realizar a comunicação da ocorrência do ataque à CONTRATANTE imediatamente após a detecção;

5.1.13.23. A solução deve permitir a proteção, no mínimo, do tráfego dos serviços;

5.1.13.24. A CONTRATADA deverá disponibilizar relatórios mensais de mitigação de ataques, contendo no mínimo horário de início do ataque, horário de início de ação de mitigação e horário de sucesso da mitigação. Em conjunto com o relatório mensal relatórios dinâmicos poderão ser disponibilizados em até 48 horas após um ataque mediante solicitação da CONTRATANTE;

5.1.13.25. A CONTRATADA terá no máximo 15 minutos para iniciar a mitigação de ataques de DOS e ANTI-DDOS;

5.1.13.26. Os serviços ofertados deverão operar no regime 24x7 (vinte e quatro horas por dia, sete dias por semana);

5.1.13.27. A solução de Gerência de Anti-DDoS deve permitir acesso a todos os recursos e módulos através de única autenticação, sem a necessidade de realizar outros logins para acessar qualquer outro recurso de

gerenciamento;

5.1.13.28. Deverá coletar métricas através de integração com a API do fabricante;

5.1.13.29. A Solução de Gerência de Anti-DDoS deverá ser operada e administrada através de uma console única, portanto, não serão aceitas soluções que possuem acessos segmentados aos módulos;

5.1.13.30. Deverá ser escalável, permitindo futuras ampliações no número de elementos de rede a serem gerenciados;

5.1.13.31. Deverá ser escalável, mas transparente para a CONTRATANTE em termos de console única;

5.1.13.32. Deverá permitir a exportação das informações para relatórios em formatos comerciais;

5.1.13.33. A Solução de Gerência de Anti-DDoS deverá fornecer, através do portal, visualização de informações on-line (em intervalos de 5 minutos e de forma gráfica) da rede que deverá apresentar, no mínimo, os seguintes itens para cada um dos elementos monitorados:

5.1.13.33.1. Tipo de ataque;

5.1.13.33.2. Volume de tráfego bloqueado e não bloqueado;

5.1.13.33.3. Origem de ataques com identificação do endereço IP e porta de origem;

5.1.13.33.4. Destino de ataques, com identificação do endereço IP e porta de destino;

5.1.13.34. Dashboards executivos com visão sumarizadas de indicadores de Anti-DDoS;

5.1.14. Fornecimento de roteador CPE

5.1.14.1. Os meios de transmissão necessários para a prestação dos serviços serão disponibilizados, através de roteador (ou através da caixa de UTM de segurança com função de roteador) e modem;

5.1.14.2. A configuração, operação e manutenção do roteador e modem serão realizadas pelos técnicos da CONTRATADA;

5.1.14.3. Os CPEs deverão suportar a velocidade do circuito de dados contratado, bem como, possuir portas e interfaces compatíveis com cada serviço.

5.2. SERVIÇOS DE SOLUÇÃO DE SEGURANÇA DE REDES NGFW TIPOS 1 e 2 - CARACTERISTICAS GERAIS

5.2.1. Solução baseada em appliance. Para maior segurança, não serão aceitos equipamentos de propósito genérico (PCs ou servidores) sobre os quais poderiam instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS-X ou GNU/Linux;

5.2.2. Poderá ser entregue em equipamento único ou com composição de equipamentos. para atender as funcionalidades exigidas;

5.2.3. Deverá possuir e estar licenciado pelo período de 60 (sessenta) meses para suporte, garantia, atualização de firmware e atualização automática de bases de dados, incluindo as seguintes funcionalidades: Firewall, TrafficShapping e QoS, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN IPSec e SSL, Controle de Aplicações, Otimização WAN, DLP – Data LeakPrevention, Controladora Wireless e Virtualização;

5.2.4. Deverá ser compatível com o item “Solução de Armazenamento de logs e Relatoria”;

5.2.5. Deverá ser compatível e gerenciado pelo item “Solução De Gerência Centralizada De Dispositivos De Segurança De Redes”;

5.2.6. Deverá estar licenciado para permitir número ilimitado de estações de rede e usuários;

5.2.7. Deverá incluir licença para a funcionalidade de VPN SSL;

5.2.8. Deverá incluir licença para atualização de vacina de antivírus/anti-spyware;

5.2.9. Deverá incluir licença de atualização para filtro de conteúdo Web;

5.2.10. Deverá incluir licença de atualização do IPS e da lista de aplicações detectadas;

5.2.11. Deverá possuir licença para número ilimitado de usuários e endereços IP;

5.2.12. Deverá possuir licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades de proteção avançada durante a vigência contratual;

5.2.13. Deverá possuir um relatório de uso de mídia social;

5.2.14. Deverá ser fornecida toda documentação técnica, bem como manual de utilização, em português do Brasil ou em inglês.

FUNCIONALIDADES DE FIREWALL

5.2.15. Deverá possuir controle de acesso à internet por endereço IP de origem e destino;

5.2.16. Deverá possuir controle de acesso à internet por subrede;

5.2.17. Deverá suportar tags de VLAN (802.1q);

5.2.18. Deverá possuir ferramenta de diagnóstico do tipo tcpdump;

5.2.19. Deverá possuir integração com servidores de autenticação RADIUS, LDAP e Microsoft Active Directory;

5.2.20. Deverá possuir integração com tokens para autenticação de 02 (dois) fatores;

5.2.21. Deverá suportar single-sign-on para Active Directory, Novell eDirectory, Citrix e RADIUS;

5.2.22. Deverá possuir métodos de autenticação de usuários para qualquer aplicação que se execute sob os protocolos TCP (HTTP, HTTPS, FTP e Telnet);

5.2.23. Deverá possuir a funcionalidade de tradução de endereços estáticos – NAT (Network AddressTranslation), um para um, vários para um, NAT64, NAT46, PAT, STUN e Full Cone NAT;

5.2.24. Deverá permitir controle de acesso à internet por períodos do dia, permitindo a aplicação de políticas por horários e por dia da semana;

5.2.25. Deverá permitir controle de acesso à internet por domínio, por exemplo: gov.br, org.br, edu.br;

5.2.26. Deverá possuir a funcionalidade de fazer tradução de endereços dinâmicos, muitos para um, PAT;

5.2.27. Deverá suportar roteamento estático e dinâmico RIP V1, V2, OSPF, ISIS e BGPv4;

5.2.28. Deverá possuir funcionalidades de DHCP Cliente, Servidor e Relay;

5.2.29. Deverá suportar aplicações multimídia, como: H.323 e SIP;

5.2.30. Deverá possuir tecnologia de firewall do tipo Statefull;

5.2.31. Deverá possuir alta disponibilidade (HA), trabalhando no esquema de redundância do tipo Ativo-Passivo e também Ativo-Ativo, com divisão de carga, com todas as licenças de software habilitadas para tal sem perda de

conexões;

5.2.32. Deverá permitir o funcionamento em modo transparente tipo “bridge” sem alterar o endereço MAC do tráfego;

5.2.33. Deverá suportar PBR – PolicyBasedRouting;

5.2.34. Deverá permitir a criação de VLANS no padrão IEEE 802.1q;

5.2.35. Deverá possuir conexão entre estação de gerência e appliance criptografada, tanto em interface gráfica, quanto em CLI (linha de comando);

5.2.36. Deverá permitir filtro de pacotes sem controle de estado (stateless) para verificação em camada 2;

5.2.37. Deverá permitir forwarding de camada 2 para protocolos não IP;

5.2.38. Deverá suportar forwardingmulticast;

5.2.39. Deverá suportar roteamento multicast PIM SparseMode e DenseMode;

5.2.40. Deverá permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos: TCP, UDP, ICMP e IP;

5.2.41. Deverá permitir o agrupamento de serviços;

5.2.42. Deverá permitir o filtro de pacotes sem a utilização de NAT;

5.2.43. Deverá permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas;

5.2.44. Deverá possuir mecanismo de anti-spoofing;

5.2.45. Deverá permitir criação de regras definidas pelo usuário;

5.2.46. Deverá permitir o serviço de autenticação para tráfego HTTP e FTP;

5.2.47. Deverá permitir IP/MAC binding, permitindo que cada endereço IP possa ser associado a um endereço MAC, gerando maior controle dos endereços internos e impedindo o IP spoofing;

5.2.48. Deverá possuir a funcionalidade de balanceamento e contingência de links;

5.2.49. Deverá suportar sFlow;

5.2.50. Solução deve ser capaz de prover Zero Touch provisioning;

5.2.51. A solução de Zero Touch provisioning deve ser capaz de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN;

5.2.52. O dispositivo 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;

5.2.53. Deverá ter a capacidade de permitir a criação de regras de firewall específicas para tipos de dispositivos identificados automaticamente (funcionalidade esta conhecida como BYOD – BringYourOwn Device), como, por exemplo: tablets, celulares e PCs, sistemas operacionais Android, Apple, Blackberry, Linux e Windows;

5.2.54. Deverá ter a capacidade de criar e aplicar políticas de reputação de cliente para registrar e pontuar as seguintes atividades: tentativas de conexões más, pacotes bloqueados por política, detecção de ataques de

intrusão, detecção de ataques de malware, atividades Web em categorias de risco, proteção de aplicação, locais geográficos que os clientes estão tentando se comunicar;

5.2.55. Deverá permitir autenticação de usuários em base local, servidor LDAP, RADIUS e TACACS;

5.2.56. Deverá permitir a criação de regras baseada em usuário, grupo de usuários, endereço IP, FQDN, tipo de dispositivo, horário, protocolo e aplicação;

5.2.57. Deverá suportar certificados X.509, SCEP, Certificate SigningRequest (CSR) e OCSP;

5.2.58. Deverá permitir funcionamento em modo bridge, router, proxy explícito, sniffer e/ou VLAN- tagged;

5.2.59. Deverá possuir mecanismo de tratamento (session-helpers ou ALGs) para os protocolos ou aplicações dcerpc, dns-tcp, dns-udp, ftp, H.245 I, H.245 0, H.323, MGCP, MMS, PMAP, PPTP, RAS, RSH, SIP, TFTP, TNS;

5.2.60. Deverá suportar SIP, H.323 e SCCP NAT Traversal;

5.2.61. Deverá permitir a criação de objetos e agrupamento de objetos de usuários, redes, FQDN, protocolos e serviços para facilitar a criação de regras;

5.2.62. Deverá possuir porta de comunicação serial ou USB para testes e configuração do equipamento, com acesso protegido por usuário e senha.

FUNCIONALIDADE DE TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO

5.2.63. Deverá 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;

5.2.64. Deverá permitir modificação de valores DSCP para o DiffServ;

5.2.65. Deverá permitir priorização de tráfego e suportar ToS;

5.2.66. Deverá limitar individualmente a banda utilizada por programas, tais como: peer-to-peer, streaming, chat, VoIP e Web;

5.2.67. Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;

5.2.68. Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP;

5.2.69. Deverá controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP;

5.2.70. Deverá permitir definir banda máxima e banda garantida para um usuário, IP, grupo de IPs, protocolo e aplicação;

5.2.71. Deverá controlar (limitar ou expandir) individualmente a banda utilizada por subrede de origem e destino;

5.2.72. Deverá controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino;

5.2.73. Deverá ter a capacidade de permitir a criação de perfis de controle de banda específicos para tipos de dispositivos identificados automaticamente (funcionalidade esta conhecida como BYOD – BringYourOwn Device), como, por exemplo: tablets, celulares e PCs, sistemas operacionais Android, Apple, Blackberry, Linux e Windows.

FUNCIONALIDADE DE ANTI-SPAM DE GATEWAY

5.2.74. Deverá permitir, na funcionalidade de AntiSpam, verificação do cabeçalho SMTP do tipo MIME;

5.2.75. Deverá possuir filtragem de e-mail por palavras chaves;

5.2.76. Deverá permitir adicionar rótulo ao assunto da mensagem quando classificado como SPAM;

5.2.77. Deverá possuir, para a funcionalidade de AntiSpam, o recurso de RBL;

5.2.78. Deverá permitir a checagem de reputação da URL no corpo mensagem de correio eletrônico;

5.2.79. Deverá ter a capacidade de permitir a criação de perfis de AntiSpam específicos para tipos de dispositivos identificados automaticamente (funcionalidade esta conhecida como BYOD – BringYourOwn Device), como, por exemplo: tablets, celulares e PCs.

FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB

5.2.80. Deverá possuir solução de filtro de conteúdo Web integrado à solução de segurança;

5.2.81. Deverá possuir, pelo menos, 70 (setenta) categorias para classificação de sites Web;

5.2.82. Deverá possuir base mínima contendo 100.000.000 (cem milhões) de sites internet Web já registrados e classificados;

5.2.83. Deverá possuir a funcionalidade de cota de tempo de utilização por categoria;

5.2.84. Deverá possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites Web, como:

5.2.84.1. Proxy anônimo;
5.2.84.2. Webmail;
5.2.84.3. Instituições de saúde;
5.2.84.4. Notícias;
5.2.84.5. Phishing;
5.2.84.6. Hackers;
5.2.84.7. Pornografia;
5.2.84.8. Racismo;
5.2.84.9. Websites pessoais;
5.2.84.10. Compras;

5.2.85. Deverá permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários;

5.2.86. Deverá permitir a criação de, pelo menos, 05 (cinco) categorias personalizadas;

5.2.87. Deverá permitir a reclassificação de sites Web, tanto por URL, quanto por endereço IP;

5.2.88. Deverá prover Termo de Responsabilidade on-line para aceite pelo usuário, a ser apresentado toda vez que houver tentativa de acesso a determinado serviço permitido ou bloqueado;

5.2.89. Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados;

5.2.90. Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;

5.2.91. Deverá possuir integração com tokens para autenticação de 02 (dois) fatores;

5.2.92. Deverá exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança;

5.2.93. Deverá 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 e activeX, através de base de URL própria atualizável;

5.2.94. Deverá permitir o bloqueio de páginas Web através da construção de filtros específicos com mecanismo de busca textual;

5.2.95. Deverá permitir a criação de listas personalizadas de URLs permitidas (lista branca) e bloqueadas (lista negra);

5.2.96. Deverá permitir o bloqueio de URLs inválidas, cujo campo CN do certificado SSL não contenha um domínio válido;

5.2.97. Deverá filtrar o conteúdo baseado em categorias em tempo real;

5.2.98. Deverá garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo Web;

5.2.99. Deverá permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP;

5.2.100. Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;

5.2.101. Deverá permitir a criação de regras para acesso/bloqueio por subrede de origem;

5.2.102. Deverá ser capaz de categorizar a página Web, tanto pela sua URL, como pelo seu endereço IP;

5.2.103. Deverá permitir o bloqueio de redirecionamento HTTP;

5.2.104. Deverá permitir o bloqueio de páginas Web por classificação como páginas que facilitem a busca de áudio, vídeo e URLs originadas de spams;

5.2.105. Deverá possuir Proxy Explícito e Transparente;

5.2.106. Deverá implementar roteamento WCCP e ICAP;

5.2.107. Deverá ter a capacidade de permitir a criação de perfis de filtragem Web específicos para tipos de dispositivos identificados automaticamente (funcionalidade esta conhecida como BYOD – BringYourOwn Device), como, por exemplo: tablets, celulares e PCs, sistemas operacionais Android, Apple, Blackberry, Linux e Windows.

FUNCIONALIDADE DE DETECÇÃO DE INTRUSÃO

5.2.108. Deverá permitir que seja definido, através de regra por IP origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão;

5.2.109. Deverá possuir base de assinaturas de IPS com, pelo menos, 3.500 (três mil e quinhentas) ameaças conhecidas;

5.2.110. Deverá estar orientado à proteção de redes;

5.2.111. Deverá permitir funcionar em modo transparente, sniffer e router;

5.2.112. Deverá possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente;

5.2.113. Deverá permitir a criação de padrões de ataque manualmente;

5.2.114. Deverá possuir integração à plataforma de segurança;

5.2.115. Deverá possuir capacidade de remontagem de pacotes para identificação de ataques;

5.2.116. 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;

5.2.117. Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias, como Denialof Service (DoS) do tipo Flood, Scan, Session e Sweep;

5.2.118. Deverá possuir mecanismos de detecção/proteção de ataques;

5.2.119. Deverá possuir reconhecimento de padrões;

5.2.120. Deverá possuir análise de protocolos;

5.2.121. Deverá possuir detecção de anomalias;

5.2.122. Deverá possuir detecção de ataques de RPC (Remote Procedure Call);

5.2.123. Deverá possuir proteção contra-ataques de Windows ou NetBios;

5.2.124. Deverá possuir proteção contra-ataques de SMTP (SimpleMessageTransferProtocol), IMAP (Internet Message Access Protocol), Sendmail ou POP (Post Office Protocol);

5.2.125. Deverá possuir proteção contra-ataques DNS (Domain Name System);

5.2.126. Deverá possuir proteção contra-ataques a FTP, SSH, Telnet e rlogin;

5.2.127. Deverá possuir proteção contra-ataques de ICMP (Internet ControlMessageProtocol);

5.2.128. Deverá possuir métodos de notificação de detecção de ataques;

5.2.129. Deverá possuir alarmes na console de administração;

5.2.130. Deverá possuir alertas via correio eletrônico;

5.2.131. Deverá possuir monitoração do comportamento do appliance, mediante SNMP. O dispositivo deverá ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede;

5.2.132. Deverá ter a capacidade de resposta/logs ativa a ataques;

5.2.133. Deverá prover a terminação de sessões via TCP resets;

5.2.134. Deverá armazenar os logs de sessões;

5.2.135. Deverá atualizar automaticamente as assinaturas para o sistema de detecção de intrusos;

5.2.136. Deverá mitigar os efeitos dos ataques de negação de serviços;

5.2.137. Deverá permitir a criação de assinaturas personalizadas;

5.2.138. Deverá possuir filtros de ataques por anomalias;

5.2.139. Deverá permitir filtros de anomalias de tráfego estatístico de: flooding, scan, source e destinationsessionlimit;

5.2.140. Deverá permitir filtros de anomalias de protocolos;

5.2.141. Deverá suportar reconhecimento de ataques de DoS, reconnaissance, exploits e evasion;

5.2.142. Deverá suportar verificação de ataque na camada de aplicação;

5.2.143. Deverá suportar verificação de tráfego em tempo real, via aceleração de hardware;

5.2.144. Deverá possuir as seguintes estratégias de bloqueio: pass, drop e reset.

FUNCIONALIDADE DE VPN

5.2.145. Deverá possuir algoritmos de criptografia para túneis VPN: AES, DES, 3DES;

5.2.146. Deverá possuir suporte a certificados PKI X.509 para construção de VPNs;

5.2.147. Deverá possuir suporte a VPNsIPSeC Site-to-Site e VPNs IPSec Client-to-Site;

5.2.148. Deverá possuir suporte a VPN SSL;

5.2.149. Deverá possuir capacidade de realizar SSL VPNs utilizando certificados digitais;

5.2.150. A VPN SSL deverá possibilitar o acesso a toda infraestrutura, de acordo com a política de segurança, através de um plug-in ActiveX e/ou Java;

5.2.151. Deverá possuir hardware acelerador criptográfico para incrementar o desempenho da VPN;

5.2.152. A VPN SSL deverá suportar cliente para plataforma Windows, Linux e Mac OS X;

5.2.153. Deverá permitir a arquitetura de VPN hub andspoke;

5.2.154. Deverá possuir suporte a inclusão em autoridades certificadoras (enrollment), mediante SCEP (Simple Certificate Enrollment Protocol) e mediante arquivos.

FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES

5.2.155. Deverá reconhecer, no mínimo, 2.000 (duas mil) aplicações;

5.2.156. Deverá possuir, pelo menos, 10 (dez) categorias para classificação de aplicações;

5.2.157. Deverá possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações, como:

5.2.157.1. P2P;
5.2.157.2. Transferência de arquivos;
5.2.157.3. VoIP;

5.2.158. Deverá permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários;

5.2.159. Deverá ser capaz de controlar aplicações independente do protocolo e porta utilizados, identificando-as apenas pelo comportamento de tráfego da mesma;

5.2.160. Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;

5.2.161. Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;

5.2.162. Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory;

5.2.163. Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP;

5.2.164. Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;

5.2.165. Deverá possuir integração com tokens para autenticação de 02 (dois) fatores;

5.2.166. Deverá permitir a criação de regras para acesso/bloqueio por subrede de origem e destino;

5.2.167. Deverá permitir a inspeção/bloqueio de códigos maliciosos para, no mínimo, as seguintes categorias: Instant Messaging e transferência de arquivos;

5.2.168. Deverá garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações;

5.2.169. Deverá permitir criação de padrões de aplicação manualmente;

FUNCIONALIDADE DE DLP (DATA LEAK PREVENTION)

5.2.170. O sistema de DLP (Data LeakPrevention – Proteção contra Vazamento de Informações) de gateway deverá funcionar de maneira que se consiga que os dados confidenciais e ou de identificação pessoal não saiam da rede e também deverá funcionar de modo que se previna que dados não requisitados entrem na sua rede;

5.2.171. Deverá inspecionar, no mínimo, os tráfegos de e-mail, HTTP, NNTP e de mensageiros instantâneos;

5.2.172. Sobre o tráfego de e-mail, deverá inspecionar, no mínimo, os protocolos SMTP, POP3 e IMAP;

5.2.173. Deverá realizar buscas para a aplicação de regras de DLP em arquivos do tipo PDF e MS- Word;

5.2.174. Deverá fazer a varredura no conteúdo de um cookie HTTP buscando por determinado texto;

5.2.175. Deverá aplicar regras baseadas em usuários autenticados, isto é, fazendo buscas pelo tráfego de um específico usuário;

5.2.176. Deverá verificar para aplicações do tipo e-mail, se o anexo das mensagens de correio entrantes/saintes possui um tamanho máximo especificado pelo administrador;

5.2.177. Deverá utilizar expressões regulares para composição das regras de verificação dos tráfegos;

5.2.178. Deverá tomar minimamente as ações de bloquear, banir usuário e colocar em quarentena a interface sobre as regras que coincidirem com o tráfego esperado pela regra;

5.2.179. Deverá permitir o armazenamento em solução específica de armazenamento de logs, o conteúdo do tráfego que coincidir com o tráfego esperado pela regra de DLP para minimamente os protocolos de e-mail, HTTP e mensageiros instantâneos;

5.2.180. Deverá permitir a composição de múltiplas regras de DLP, formando uma regra única mais específica que usa lógica booleana para fazer a comparação com o tráfego que atravessa o sistema.

FUNCIONALIDADE DE BALANCEAMENTO DE CARGA

5.2.181. Deverá permitir a criação de endereços IPs virtuais;

5.2.182. Deverá permitir balanceamento de carga entre, pelo menos, 04 (quatro) servidores reais;

5.2.183. Deverá suportar balanceamento, ao menos, para os seguintes serviços: HTTP, HTTPS, TCP e UDP;

5.2.184. Deverá permitir balanceamento, ao menos, com os seguintes métodos: Hash do endereço IP de origem, Round Robin, Weighted, FirstAlive e HTTP host;

5.2.185. Deverá permitir persistência de sessão por cookie HTTP ou SSL session ID;

5.2.186. Deverá permitir que seja mantido o IP de origem;

5.2.187. Deverá suportar SSL offloading nos equipamentos que suportem, pelo menos, 200 (duzentos) usuários;

5.2.188. Deverá ter a capacidade de identificar, através de healthchecks, quais os servidores que estejam ativos, removendo automaticamente o tráfego dos servidores que não estejam;

5.2.189. Deverá permitir que o healthcheck seja feito, ao menos, via ICMP, TCP em porta configurável e HTTP em URL configurável.

FUNCIONALIDADE DE VIRTUALIZAÇÃO

5.2.190. Deverá suportar a criação de, ao menos, 10 (dez) instâncias virtuais no mesmo hardware;

5.2.191. Deverá permitir a criação de administradores independentes para cada uma das instâncias virtuais;

5.2.192. Deverá permitir a criação de um administrador global que tenha acesso a todas as configurações das instâncias virtuais criadas.

FUNCIONALIDADE DE CONTROLADORA WIRELESS

5.2.193. Deverá ser capaz de gerenciar, de forma centralizada, Pontos de Acesso do mesmo fabricante;

5.2.194. Deverá suportar o serviço de servidor DHCP por SSID para prover endereçamento IP automático para os clientes wireless;

5.2.195. Deverá suportar monitoração e supressão de Ponto de Acesso indevido;

5.2.196. Deverá prover autenticação para a rede wireless através de bases externas, como: LDAP, RADIUS ou TACACS+;

5.2.197. Deverá permitir a visualização dos clientes conectados;

5.2.198. Deverá prover suporte a Fast Roaming;

5.2.199. Deverá ajustar automaticamente os canais de modo a otimizar a cobertura de rede e mudar as condições de RF;

5.2.200. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência;

5.2.201. Deverá possuir Captive Portal por SSID;

5.2.202. Deverá permitir configurar o bloqueio de tráfego entre SSIDs;

5.2.203. Deverá suportar Wi-Fi Protected Access (WPA), WPA2 ou WPA3 por SSID, utilizando-se de AES e/ou TKIP;

5.2.204. Deverá suportar os seguintes métodos de autenticação EAP:

5.2.204.1. EAP-TLS
5.2.204.2. EAP-TTLS;
5.2.204.3. EAP-PEAP;
5.2.204.4. EAP-SIM
5.2.204.5. EAP-AKA;

5.2.205. Deverá suportar 802.1x através de RADIUS;

5.2.206. Deverá suportar filtro baseado em endereço MAC por SSID;

5.2.207. Deverá permitir configurar parâmetros de rádio, como: banda e canal;

5.2.208. Deverá possuir método de descoberta de novos Pontos de Acesso baseados em Broadcast ou Multicast;

5.2.209. Deverá possuir mecanismo de identificação e controle de rogue APs, suportando supressão automática e bloqueio por endereço MAC de APs;

5.2.210. Deverá possuir lista contendo Pontos de Acesso Aceitos e Pontos de Acesso Indevidos (Rogue);

5.2.211. Deverá possuir WIDS com, ao menos, os seguintes perfis:

5.2.211.1. Rogue/Interfering AP Detection;
5.2.211.2. Ad-hoc Network Detection;
5.2.211.3. Wireless Bridge Detection;
5.2.211.4. Weak WEP Detection;
5.2.211.5. MAC OUI Checking;

5.2.212. Deverá permitir o uso de voz e dados sobre um mesmo SSID;

5.2.213. A solução deverá detectar Receiver Start ofPacket (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm;

5.2.214. A controladora deverá oferecer Firewall integrado, baseado em identidade do usuário;

5.2.215. Deverá possuir controle baseado em política de firewall para acesso entre as WLANs;

5.2.216. Deverá permitir a criação de políticas de trafficshaping;

5.2.217. Deverá permitir a criação de políticas de firewall baseadas em horário;

5.2.218. Deverá permitir NAT nas políticas de firewall;

5.2.219. Deverá possibilitar definir número de clientes por SSID;

5.2.220. Deverá permitir e/ou bloquear o tráfego entre SSIDs;

5.2.221. Deverá possuir mecanismo de criação automática de usuários visitantes e senhas autogeradas e/ou manual, que possam ser enviadas por e-mail ou SMS aos usuários, e com capacidade de definição de horário da expiração da senha;

5.2.222. A comunicação entre o Access Point e a Controladora Wireless deverá poder ser efetuada de forma criptografada;

5.2.223. Deverá possuir mecanismo de ajuste de potência do sinal, de forma a reduzir interferência entre canais entre 02 (dois) Access Points gerenciados;

5.2.224. Deverá possuir mecanismo de balanceamento de tráfego/usuários entre Access Points;

5.2.225. Deverá possuir mecanismo de balanceamento de tráfego/usuários entre frequências e/ou

5.2.226. rádios;

5.2.227. Toda a configuração do Ponto de Acesso deverá ser executada através da Controladora Wireless;

5.2.228. Deverá permitir a identificação de APs com firmware desatualizado e efetuar o upgrade via interface gráfica;

5.2.229. Deverá possuir console de monitoramento dos usuários conectados, indicando em que Access Point, em que rádio, em que canal, endereço IP do usuário, tipo de dispositivo e sistema operacional, uso de banda, potência do sinal e relação sinal/ruído;

5.2.230. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser encaminhados dentro do túnel até o controlador wireless. Caso o controlador wireless não seja capaz de operar gerenciando os pontos de acesso e concentrando o tráfego tunelado simultaneamente, então a solução ofertada deve ser composta com elemento adicional do próprio fabricante para suportar a conexão dos túneis originados dos pontos de acesso;

5.2.231. A Controladora deverá oferecer Firewall integrado, baseado em identidade do usuário, entre todas as redes cujo tráfego seja tunelado até a Controladora;

5.2.232. Deverá possuir controle baseado em política de firewall para acesso entre as WLANs cujo tráfego seja tunelado até a Controladora;

5.2.233. Deverá permitir a criação de políticas de trafficshaping entre todas as redes cujo tráfego seja tunelado até a Controladora;

5.2.234. Deverá permitir aplicar políticas de filtro de conteúdo Web, que seja baseado em categorias de sites automaticamente atualizadas, para todas as redes cujo tráfego seja tunelado até a Controladora;

5.2.235. Deverá permitir aplicar políticas de antivírus, com detecção e bloqueio de malwares e redes botnet, entre todas as redes cujo tráfego seja tunelado até a Controladora;

5.2.236. Deverá permitir aplicar políticas de IPS, bloqueando e/ou monitorando tentativas de ataques, com base de assinatura de ataques atualizada automaticamente, entre todas as redes cujo tráfego seja tunelado até a Controladora;

5.2.237. Deverá permitir aplicar políticas de controle AntiSpam para todas as redes cujo tráfego seja tunelado até a Controladora;

5.2.238. Deverá permitir controlar, identificar e bloquear tráfego de aplicações do tipo P2P, IM, Chat, Redes Sociais, Skype, Proxies Anônimos, streamings de áudio e vídeo, jogos entre outros, e que seja baseado no padrão de comunicação de tais aplicações, entre todas as redes cujo tráfego seja tunelado até a Controladora;

5.2.239. A solução deve implementar recurso de controle de acesso à rede (NAC - Network Access Control), identificando automaticamente o tipo de equipamento conectado (profiling) e atribuindo de maneira automática a política de acesso à rede;

FUNCIONALIDADE DE CONTROLADORA DE SWITCH

5.2.240. Deverá ser capaz de gerenciar, de forma centralizada, Switches do mesmo fabricante;

5.2.241. Deve operar como ponto central para automação e gerenciamento dos switches;

5.2.242. Deve realizar o gerenciamento de inventário de hardware, software e configuração dos Switches;

5.2.243. Deve possuir interface gráfica para configuração, administração e monitoração dos switches;

5.2.244. Deve apresentar graficamente a topologia da rede com todos os switches administrados para monitoramento, além de ilustrar graficamente status dos uplinks e dos equipamentos para identificação de eventuais problemas na rede;

5.2.245. Deve montar a topologia da rede de maneira automática;

5.2.246. Deve ser capaz de configurar os switches da rede;

5.2.247. Deve através da interface gráfica deve ser capaz de configurar as VLANs da rede e distribui-las automaticamente em todos os switches gerenciados;

5.2.248. Deve através da interface gráfica deve ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches;

5.2.249. Deve através da interface gráfica deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches;

5.2.250. Deve através da interface gráfica deve ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches;

5.2.251. Através da interface gráfica deve ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches;

5.2.252. Deve através da interface gráfica deve ser capaz de realizar configurações do protocolo SpanningTree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard;

5.2.253. Deve através da interface gráfica deve ser capaz de aplicar políticas de segurança e controle de tráfego para filtrar o tráfego da rede;

5.2.254. A solução de gerência centralizada deve ser capaz de identificar as aplicações acessadas na rede através de análise DPI (DeepPacketInspection);

5.2.255. Deve ser capaz de configurar parâmetros SNMP dos switches;

5.2.256. A solução de gerência centralizada deve gerenciar as atualizações de firmware (software) dos switches gerenciados, recomendando versões de software para cada switch, além de permitir a atualização dos switches individualmente;

5.2.257. A solução de gerência centralizada deve permitir o envio automático de e-mails de notificação para os administradores da rede em caso de eventos de falhas;

5.2.258. Solução de gerência centralizada deve apresentar graficamente informações sobre erros nas interfaces dos switches;

5.2.259. A solução deve apresentar graficamente informações sobre disponibilidade dos switches;

5.2.260. Deve prover indicadores de saúde dos elementos críticos do ambiente;

5.2.261. Deve registrar eventos para auditoria de todos os acessos e mudanças de configuração realizadas por usuários;

5.2.262. Deve realizar as funções de gerenciamento de falhas e eventos dos switches da rede;

5.2.263. Deve possuir API no formato REST;

FUNCIONALIDADE DE SD-WAN

5.2.264. A solução SD-WAN deve ser viabilizada com recursos de segurança integrados de: Firewall, VPN, Antivírus, IPS e Filtro de Segurança Web;

5.2.265. A solução SD-WAN deve suportar NAT em contexto de saída (Nat Outbound) para um pool de IPs

públicos;

5.2.266. A solução SD-WAN deve suportar micro-segmentação de tráfego onde seja possível aplicar políticas de IPS e Antivírus entre segmentos de LAN;

5.2.267. A solução SD-WAN deve prover capacidade de inspeção SSL para a inspeção de tráfego https nas filiais, no contexto: bloqueio de malwares e reconhecimento em camada 7 de aplicações;

5.2.268. Solução deve ser capaz de prover uma arquitetura onde em uma comunicação Matriz x Filiais, em que a comunicação de uma Filial A para a Matriz esteja comprometida, possa ser utilizada a comunicação entre Filial B e Matriz, em que através deste circuito, a Filial A alcance a Matriz;

5.2.269. A solução deve ser capaz de criar VPN "Full-Mesh" em interface Gráfica, de forma automática, e sem que o administrador precise configurar site por site;

5.2.270. A configuração VPN IPSEC deverá oferecer suporte para DH Group: 14 e 15;

5.2.271. Reconhecimento em camada 7 totalmente segregado da camada 4;

5.2.272. Deve de forma alternativa, contar com um banco de Dados interno, onde seja possível atrelar uma aplicação à um determinado IP/ range de IPs de destino;

5.2.273. O reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;

5.2.274. Ainda sobre o reconhecimento de Aplicações, a solução deve fornecer o reconhecimento default em camada 7, de pelo menos mais de 2000 aplicações largamente utilizadas em contextos de SaaS, Aplicações na Nuvem, Aplicações Multimídia (Vimeo, YouTube, Facebook, etc);

5.2.275. A solução de SD-WAN deve suportar Roteamento dinâmico BGP com suporte a IPv6;

5.2.276. A solução deve ser capaz de refletir, de forma manual ou automatizada, suas políticas de SD-WAN em condições onde a largura de banda é modificada;

5.2.277. A solução deve ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jitter e PacketLoss, onde seja possível configurar um valor de Theshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN;

5.2.278. A solução deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorrerá quando o link principal recuperado seja X% (com X variando de 10 à 50) do seu valor de Saúde melhor que o link atual;

5.2.279. A solução deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorra dentro de um espaço de tempo de X segundos, configurável pelo administrador do sistema;

5.2.280. A solução deve permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da Interface SD-WAN.

5.3. SOLUÇÃO DE SEGURANÇA DE REDES NGFW TIPO 1 - CARACTERISTICAS ESPECÍFICAS:

5.3.1. Deverá possuir fonte de alimentação com chaveamento automático 110/220V redundante Hot Swappable. A fonte fornecida deverá suportar sozinha a operação da unidade com todos os módulos de interface ativos;

5.3.2. Firewall com capacidade mínima de processamento de 18 (dezoito) Gbps;

5.3.3. IPS com capacidade mínima de processamento de 11 (onze) Gbps;

5.3.4. Proteção a ameaças avançadas, isto é, com as funções de Firewall, IPS, controle de aplicação e proteção de Malware/Antivírus ativadas, com capacidade mínima de processamento de 1 (um) Gbps. Caso o fabricante divulgue

múltiplos valores para este requisito, somente o de menor valor será aceito;

5.3.5. Inspeção SSL Throughput com capacidade mínima de processamento de 1 (um) Gbps;

5.3.6. VPN com capacidade de, pelo menos, 10 (dez) Gbps de tráfego IPSec;

5.3.7. VPN SSL com capacidade de, pelo menos, 1 (um) Gbps de tráfego;

5.3.8. Deverá suportar 1.500.000 (um milhão e quinhentos mil) conexões simultâneas;

5.3.9. Deverão ser licenciados para suportar, pelo menos, 500 (quinhantos) usuários de VPN SSL;

5.3.10. Deverá suportar, pelo menos, 56.000 (cinquenta e seis mil) novas conexões por segundo;

5.3.11. Deverá suportar, pelo menos, 2.000 (dois mil) túneis de VPN Site-Site;

5.3.12. Deverá suportar, pelo menos, 15.000 (quinze mil) túneis de VPN Client-Site;

5.3.13. Deverá suportar, pelo menos, 02 (duas) interfaces SFP+ 10GE;

5.3.14. Deverá possuir, pelo menos, 12 (doze) interfaces RJ 45;

5.3.15. Deverá possuir porta USB para conexão de modem 3G/4G;

5.3.16. Deverá ser capaz de gerenciar, via funcionalidade de Controladora Wireless, ao menos, 100 (quinhentos) Pontos de Acesso sem fio;

5.3.17. Deverá ser capaz de gerenciar, via funcionalidade de Controladora Switch, ao menos, 30 (trinta) equipamentos.

5.4. SOLUÇÃO DE SEGURANÇA DE REDES NGFW TIPO 2 - CARACTERISTICAS ESPECÍFICAS:

5.4.1. Deverá possuir fonte de alimentação com chaveamento automático 110/220V redundante. A fonte fornecida deverá suportar sozinha a operação da unidade com todos os módulos de interface ativos;

5.4.2. Firewall com capacidade mínima de processamento de 10 (dez) Gbps;

5.4.3. IPS com capacidade mínima de processamento de 1.4 (um ponto quatro) Gbps;

5.4.4. Proteção a ameaças avançadas, isto é, com as funções de Firewall, IPS, controle de aplicação e proteção de Malware/Antivírus ativadas, com capacidade mínima de processamento de 0.7 Gbps. Caso o fabricante divulgue múltiplos valores para este requisito, somente o de menor valor será aceito;

5.4.5. Inspeção SSL Throughput com capacidade mínima de processamento de 0.9 Gbps;

5.4.6. VPN com capacidade de, pelo menos, 6 (seis) Gbps de tráfego IPSec;

5.4.7. VPN SSL com capacidade de, pelo menos, 0.9 Gbps de tráfego;

5.4.8. Deverá suportar 700.000 (setecentos mil) conexões simultâneas;

5.4.9. Deverão ser licenciados para suportar, pelo menos, 200 (duzentos) usuários de VPN SSL;

5.4.10. Deverá suportar, pelo menos, 35.000 (trinta e cinco mil) novas conexões por segundo;

5.4.11. Deverá suportar, pelo menos, 200 (duzentosl) túneis de VPN Site-Site;

5.4.12. Deverá suportar, pelo menos, 500 (quinhentos) túneis de VPN Client-Site;

5.4.13. Deverá possuir, pelo menos, 5 (cinco) interfaces RJ 45;

5.4.14. Deverá possuir porta USB para conexão de modem 3G/4G;

5.4.15. Deverá ser capaz de gerenciar, via funcionalidade de Controladora Wireless, ao menos, 64 (sessenta e quatro) Pontos de Acesso sem fio;

5.4.16. Deverá ser capaz de gerenciar, via funcionalidade de Controladora Switch, ao menos, 20(vinte) equipamentos.

5.5. SERVIÇOS DE SOLUÇÃO DE CONTROLE DE ACESSO A REDE (NAC)

5.5.1. Solução de controle de acesso à rede, a ser ofertado em formato de appliance físico ou virtual, este que deverá estar disponível para as plataformas Vmware ESXi, AWS e Microsoft Azure;

5.5.2. Deve ser uma solução multi-vendor capaz de suportar os switches e concentrador VPN do orgão;

5.5.3. Deve suportar variadas soluções de Wi-Fi do mercado, tais como: Aruba, Ruckus, Cisco, Fortinet, Aerohive e Enterasys, pelo menos;

5.5.4. A solução deve suportar capacidade de expansão para até 2000 (duas mil) portas de rede, sem demandar do cliente a troca do hardware ou VM;

5.5.5. Caso a solução seja entregue em hardware, deve ser provida com alta disponibilidade;

5.5.6. Deverá possuir licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades descritas neste termo pelo período de 60 (sessenta) meses;

5.5.7. Deverá suportar um mínimo de 600 endpoints;

5.5.8. A solução deve ser capaz de inspecionar tanto IoT quanto estações/notebooks, sem depender de recursos como 802.1X e Mac-address bypass (MAB);

5.5.9. Para estações de trabalho, deve suportar verificação de compliance em VPN IPsec e SSL;

5.5.10. A licença contemplada deverá suportar todas as características exigidas neste termo de referência;

5.5.11. A solução deve permitir diferentes perfis de administração, com a capacidade de limitar e controlar a quantidade de acesso permitido às funcionalidades disponíveis, dependendo do grupo administrativo da organização ao qual o usuário pertence;

5.5.12. Deve detectar e classificar automaticamente o tipo dos dispositivos conectados na rede sem a necessidade de softwares instalados nos dispositivos;

5.5.13. Deve permitir determinar o perfil dos dispositivos descobertos por meio de métodos que não exigem a instalação de agentes, incluindo pelo menos os seguintes:

5.5.14. DHCP Fingerprint;

5.5.14.1. Consultas via protocolo HTTP/HTTPS;
5.5.14.2.Consultas via protocolo SNMP;
5.5.14.3.Consultas via protocolo SSH;
5.5.14.4.Consultas via protocolo Telnet;
5.5.14.5.Consultas de portas TCP;
5.5.14.6.Consultas de portas UDP;
5.5.14.7.MAC OUI;
5.5.14.8.Consultas via protocolo WMI;

5.5.14.9.Protocolo ONVIF;
5.5.14.10.Base assinaturas pré-definidas;

5.5.15. A solução deve ser capaz de reconhecer as seguintes informações sobre os dispositivos conectados à rede:

5.5.15.1. Endereço MAC;
5.5.15.2. Endereço IP;
5.5.15.3. Sistema operacional;
5.5.15.4. Nome do host;
5.5.15.5. Horário de conexão;
5.5.15.6. Usuário conectado;
5.5.15.7. Localização.

5.5.16. A solução deve ser capaz de reconhecer os seguintes sistemas operacionais em execução nos dispositivos conectados à rede:

5.5.16.1. Android;
5.5.16.2. Apple iOS para iPhone, iPod e iPad;
5.5.16.3. Chrome OS;
5.5.16.4. Linux;
5.5.16.5. MacOS X;
5.5.16.6. Windows 7, 8 e 10;

5.5.17. Deve lembrar o perfil atribuído a cada dispositivo e verificar sua validade a cada conexão;

5.5.18. Deve permitir a designação de um sponsor para autorizar a categorização dos dispositivos;

5.5.19. Deve permitir a recategorização periódica de dispositivos;

5.5.20. Deve permitir a importação de um arquivo CSV contendo informações sobre os dispositivos a serem registrados;

5.5.21. A solução deve incluir a detecção de dispositivos desconhecidos conectados à rede e adotar medidas de controle para limitar o acesso;

5.5.22. A solução deve suportar autenticação através de EAP-PEAP e EAP-TLS;

5.5.23. A solução deve suportar RADIUS Change of Authorization;

5.5.24. A solução deve suportar MAC Address Bypass;

5.5.25. A solução deve consultar bases LDAP e Active Directory para a identificação de usuários e grupos de usuários;

5.5.26. A solução deve permitir a criação de políticas de controle que combinem informações sobre a identidade do usuário e tipo de dispositivo com objetivo de autorizar dinâmicamente o acesso à rede;

5.5.27. Deve permitir a definição dos horários em que os dispositivos serão autorizados a conectar na rede;

5.5.28. Deve garantir a segmentação dinâmica da rede e aplicação de políticas de segurança, tendo como base variadas combinações, como login do AD e atributos (departamento, cidade, email, telefone), características da máquina (asset tag, hostname), localidade e horário;

5.5.29. A solução deve incluir recursos de gerenciamento de visitantes, permitindo a criação de diferentes perfis de utilização e autorização a serem associados aos usuários, distinguindo por exemplo prestadores de serviços dos visitantes;

5.5.30. A solução deve permitir o cadastro dos usuários visitantes na base interna da ferramenta para que não seja

necessário realizar consultas em bases externas;

5.5.31. A solução deve possuir ferramenta que permita a geração automática de credenciais para usuários visitantes com login e respectivas senhas;

5.5.32. A solução deve possuir ferramenta que permita a criação de credenciais para eventos;

5.5.33. Deve permitir a definição de complexidade da senha dos usuários visitantes;

5.5.34. Deve ser possível definir um período de validade para as contas de usuários visitantes;

5.5.35. Deve ser possível definir data e horário para início e encerramento das contas de usuários visitantes;

5.5.36. A autenticação e autorização dos usuários visitantes deve ocorrer através de portal captivo acessível via browser web;

5.5.37. Os visitantes em hipótese alguma deverão ter acesso à Internet e rede interna antes que a autenticação seja concluída e o usuário seja autorizado;

5.5.38. A solução deve vincular o login do visitante à máquina utilizada no acesso;

5.5.39. Deve suportar a validação de credenciais:

5.5.39.1. Em base local interna à ferramenta;
5.5.39.2. Em servidores RADIUS;
5.5.39.3. Em servidores LDAP;

5.5.40. A ferramenta deve permitir que os usuários visitantes possam realizar auto-registro através do preenchimento de cadastro disponível em portal web;

5.5.41. Deve permitir a customização dos campos obrigatórios e opcionais para o cadastro de auto-registro;

5.5.42. A solução deve suportar o envio da senha de acesso aos visitantes através de SMS e e-mail;

5.5.43. Deve ser possível definir um período para que os usuários visitantes sejam obrigados a se reautenticar;

5.5.44. Deve permitir a designação de grupos de usuários com função de sponsor que ficarão responsáveis por autorizar o acesso dos usuários visitantes e prestadores de serviços;

5.5.45. Os usuários do tipo sponsor poderão cadastrar previamente um usuário visitante. O portal de cadastro e gerenciamento de usuários visitantes não deve permtir gerência administrativa dos demais recursos da solução;

5.5.46. A solução deve permitir a customização da aparência do captive portal, permitindo editar textos e inserir imagens;

5.5.47. Os usuários do tipo sponsor podem ser cadastrados na base local da ferramenta ou fazer parte de grupo de usuários em base LDAP/Active Directory;

5.5.48. A solução deve incluir recursos de conformidade de endpoint. Antes de permitir que os dispositivos acessem a rede, a solução deve garantir que estes cumpram requisitos de segurança, integridade e conformidade;

5.5.49. Deve permitir o uso de software agente instalado no dispositivo e agentes evanescentes que não precisam ser instalados;

5.5.50. Tanto para IoTs quanto para estações de trabalho, se configurado, não devem ter qualquer acesso à rede de produção enquanto não forem inspecionados e identificados;

5.5.51. Se um dispositivo não passar os testes de conformidade, deve ser possível:

5.5.51.1. Não forçar a remediação;
5.5.51.2. Forçar a remediação imediatamente enviando o dispositivo à rede de quarentena;
5.5.51.3. Permitir a remediação retardada, ou seja, dando um período de tolerância para que o usuário corrija o problema. Caso os problemas persistam, o dispositivo deve ser colocado em quarentena;

5.5.52. A solução deve permitir verificações de conformidade em endpoints que façam uso do sistema operacional:

5.5.52.1. Windows 7;
5.5.52.2. Windows 8;
5.5.52.3. Windows 10;
5.5.52.4. MacOS;
5.5.52.5. Linux.

5.5.53. Para garantir a conformidade com as políticas de segurança, a solução deve permitir que sejam verificados os seguintes itens antes de autorizar o acesso de um endpoint na rede:

5.5.53.1. Presença de software de anti-vírus instalado e em execução;
5.5.53.2. Versão do sistema operacional;
5.5.53.3. Nome de domínio do Active Directory ao qual a estação Windows pertença;
5.5.53.4. Serviços em execução para estações Windows;
5.5.53.5. Informações sobre um determinado certificado digital em estações Windows;
5.5.53.6. Registros ou chaves de registro para estações Windows;
5.5.53.7. Processos em execução para estações Windows, Linux e MacOS;
5.5.53.8. Arquivo armazenado em um determinado diretório para estações Windows, Linux e MacOS;
5.5.53.9. Pacotes instalados em estações Linux e MacOS.

5.5.54. A solução deve ser capaz de monitorar quando um serviço requirido for desabilitado ou interrompido em computadores. Além disso deve enviar a estação para quarentena de forma a garantir a conformidade com a política de segurança;

5.5.55. Deve possuir serviço RADIUS interno, além de permitir o uso de RADIUS externos;

5.5.56. Deve permitir a distribuição de agentes através de, pelo menos, os seguintes métodos:

5.5.56.1. Programas de gerenciamento e distribuição de software;
5.5.66.2. GPO do Active Directory;
5.5.56.3. Captive Portal;

5.5.57. Deve permitir a atualização automática ou programada dos agentes instalados nas máquinas;

5.5.58. O agente instalado nos computadores deve notificar os usuários com mensagens informativas em casos de eventos;

5.5.59. Quando em quarentena, um portal web deve ser apresentado aos usuários com informações sobre as razões pelas quais estes foram movidos para o isolamento;

5.5.60. A solução deve compartilhar a identificação dos usuários e/ou dispositivos autenticados para a plataforma de segurança da rede via SSO, de forma que sejam vinculadas aos acessos de Internet, provendo rastreabilidade futura;

5.5.61. No que tange compliance, quando houver sucesso, falha ou alerta, a solução deve permitir as seguintes ações: alerta, envio de email e SMS, desabilitar o host, envio de mensagem direta para o host envolvido e executar políticas adicionais de compliance;

5.5.62. A solução deve integrar com plataformas de MDM, suportando pelo menos: FortiClient, In Tune, Mobile Iron e Air Watch;

5.5.63. Deve suportar integração com soluções de patching;

5.5.64. Deve suportar integração com soluções de análise de vulnerabilidades;

5.5.65. A solução deve possuir dashboard que apresente informações e estatísticas relevantes de forma resumida;

5.5.66. A solução deve permitir a customização do dashboard para apresentar as informações que o administrador considera relevante;

5.5.67. A solução deve permitir a consulta de informações e alteração de parâmetros de configuração via REST API;

5.5.68. A solução deve armazenar os eventos internamente e permitir que sejam exportados;

5.5.69. A solução deve permitir a exportação dos eventos através de syslog;

5.5.70. Deve suportar alta disponibilidade, suportando todos os registros e autenticações caso um nó da solução esteja indisponível;

5.5.71. A solução deve ser capaz de isolar hosts na quarentena mesmo quando estes estão conectados em redes de localidades remotas, tais como filiais. Não deve ser necessário estender a VLAN para isso;

5.5.72. Deve possuir registro dos eventos ocorridos na solução, bem como auditoria das configurações efetuadas;

5.5.73. Deve possibilitar o rastreio de dispositivos, notificando a localização deles quando se conectarem à rede;

5.5.74. Dentre os relatórios disponibilizados pela solução dedicada de logs, deve suportar relatórios listando os endpoints por localidade e fabricante, usuários associados, além de relatórios de inventário, devices registrados e rogues;

5.6. Solução de segurança de aplicações WEB e API - Firewall de Aplicação (WAF)

5.6.1. A solução deverá ser fornecida em sua integralidade, com todos os elementos de hardware/software necessários à sua implantação, inclusive licenças de sistemas operacionais, bancos de dados e outros softwares que se fizerem necessários à implantação da solução.

5.6.2. Solução de segurança de aplicações WEB e API Firewall de Aplicação (WAF)

5.6.2.1. Os serviços de manutenção e suporte técnico devem ser fornecidos pelo período de 36 (trinta e seis meses).

Especificações Técnicas:

5.6.3. Requisitos Mínimos de Performance:

5.6.3.1. Deve ser do tipo appliance físico com software e recurso dedicado à função de Firewall de Aplicação (WAF);

5.6.3.2. Deve possuir throughput mínimo para HTTP de 250 mbps;

5.6.3.3. Deve introduzir latência inferior a 5 milissegundos, a fim de não impactar o desempenho das aplicações Web;

5.6.3.4. Deve suportar quantidade ilimitada de aplicações protegidas;

5.6.3.5. Deve possuir 04 (quatro) interfaces 1GE RJ45;

5.6.3.6. Deve possuir 04 (quatro) interfaces 1GE SFP;

5.6.3.7. Deve possuir 1 (uma) Interface Ethernet RJ45 10/100/1000 dedicada para gerenciamento;

5.6.3.8. Possuir área de armazenamento interno de no mínimo 480 GB SSD;

5.6.3.9. Deve suportar no mínimo 30 (trinta) instâncias administrativas independentes entre si, permitindo criar níveis diferentes de privilégios de acesso dos administradores;

5.6.3.10. Deve suportar no mínimo 62 políticas de servidores;

5.6.3.11. Deve suportar no mínimo 250 grupos ou pools de servidores, e cada pool deve suportar no mínimo 1000 membros;

5.6.3.12. Requisitos Mínimos de Funcionalidades

5.6.3.13. A solução deverá ser entregue em appliance físico e o equipamento deverá ser instalado em local a ser definido pela CONTRATANTE, devendo estar licenciado e ser compatível para atender os requisitos de performance da solução;

5.6.3.14. O licenciamento de todos os recursos solicitados deve ser do tipo perpétuo;

5.6.3.15. A solução fornecida deve prover redundância e alta disponibilidade, nos modos ativo-standby e ativo-ativo (Clustering);

5.6.3.16. Funcionalidades de Rede

5.6.3.17. A solução deve ser capaz de ser implementada no modo Proxy (Transparente e Reverso), Passivo, ou “Sniffer” (Offline) e Inline Transparente (Bridge);

5.6.3.18. A solução deve ser capaz de ser implementada com protocolo WCCP.

5.6.3.19. Suportar VLANs no padrão IEEE 802.1q;

5.6.3.20. Deve implementar o protocolo de negociação Link Aggregation Control Protocol (LACP) IEEE 802.3ad;

5.6.3.21. Suportar endereçamento IPv4 e IPv6 nas interfaces físicas e virtuais (VLANs);

5.6.3.22. A solução deve suportar roteamento por política (policy route);

5.6.3.23. Funcionalidades de Gerência

5.6.3.24. O sistema operacional / firmware deve suportar interface gráfica web para a configuração das funções do sistema operacional, utilizando navegadores disponíveis gratuitamente e protocolo HTTPS, e através de CLI (interface de linha de comando), acessando localmente, via porta de console, ou remotamente via SSH;

5.6.3.25. Deve possuir administração baseada em interface web HTTPS;

5.6.3.26. Possuir auto-complementação de comandos na CLI;

5.6.3.27. Possuir ajuda contextual na CLI;

5.6.3.28. A solução deve possuir Interface Gráfica com informações sobre o sistema Ex: (Informações do Cluster, hostname, número de série, modo de operação, tempo em serviço, versão do firmware);

5.6.3.29. Deverá ser possível visualizar através da interface gráfica de gerência informações de licenças e assinaturas;

5.6.3.30. Deve prover, na interface de gerência, as seguintes informações do sistema para cada gateway:

5.6.3.31. Consumo de CPU e estatísticas das conexões;

5.6.3.32. Deve ser possível visualizar na interface de gerência as informações de consumo de memória;

5.6.3.33. Deve ser possível visualizar na interface de gerência ou CLI as informações de utilização de disco de log;

5.6.3.34. Deverá possuir ferramenta, na interface gráfica de gerência (dashboard) que permita visualizar os últimos logs de ataque detectados/bloqueados;

5.6.3.35. Deve prover as seguintes informações, na interface de gráfica de gerência: estatísticas de throughput HTTP em tempo real, estatísticas dos eventos de ataque detectados/bloqueados, estatísticas de requisições HTTP em tempo real e últimos logs de eventos do sistema;

5.6.3.36. Possuir na interface gráfica estatísticas de conexões concorrentes e por segundo, de políticas de segurança do sistema.

5.6.3.37. Possuir um painel de visualização com informações das interfaces de rede do sistema;

5.6.3.38. A configuração de administração da solução deve possibilitar a utilização de perfis;

5.6.3.39. Deve ser possível executar e restaurar backup via interface Web (GUI);

5.6.3.40. Deve ter a opção para criptografar o backup;

5.6.3.41. Deve ser possível executar e restaurar backup utilizando-se um ou mais dos seguintes protocolos: FTP, SFTP, TFTP ou HTTPS;

5.6.3.42. Deve ser possível instalar um firmware alternativo em disco e inicializá-lo em caso de falha do firmware principal;

5.6.3.43. Deve ter suporte ao protocolo de monitoração SNMP v1, SNMP v2c e SNMP v3;

5.6.3.44. Deve ser capaz de realizar notificações de eventos de segurança através de e-mail, traps SNMP e Syslog;

5.6.3.45. A solução deverá ter a capacidade de armazenar logs localmente em disco e em servidor externo via protocolo SYSLOG;

5.6.3.46. Ter a capacidade de armazenar logs em appliance remoto;

5.6.3.47. A solução deve ter a capacidade de adicionar identificadores customizados nos registros syslog antes de envio, como hostname, atrelados a valores fixos ou variáveis;

5.6.3.48. A solução deve ter a capacidade de enviar alertas por e-mail de eventos baseados em severidades e/ou categorias;

5.6.3.49. A solução deve possuir dados analíticos contendo localização geográfica dos clientes web;

5.6.3.50. A solução deve possuir dados analíticos, sendo possível visualizar a contagem total de ataques e percentual de cada país de origem, o volume total de tráfego em bytes e percentual de cada país de origem e o total de acessos (hits) e percentual de cada país de origem;

5.6.3.51. Deverá ter a capacidade de gerar relatórios detalhados baseados em tráfego/acessos/atividades do usuário;

5.6.3.52. Deve ter suporte a RESTful API para gerenciamento de configurações;

5.6.3.53. Deve suportar todas as funcionalidades para comunicação HTTP/2;

5.6.3.54. Funcionalidades de Autenticação

5.6.3.55. Os usuários devem ser capazes de autenticar através do cabeçalho de autorização HTTP /HTTPS;

5.6.3.56. Os usuários devem ser capazes de autenticar através de formulários HTML embutidos;

5.6.3.57. A solução deverá ser capaz de autenticar usuários através de certificados digitais pessoais;

5.6.3.58. Deve possuir base local para armazenamento e autenticação contas de usuários;

5.6.3.59. A solução deve ter a capacidade de autenticar usuários em bases externas/remotas LDAP e RADIUS;

5.6.3.60. Os usuários devem ser capazes de autenticar através de contas de usuários em base remota NTLM;

5.6.3.61 .A solução deve ser capaz de criar grupos de usuários para acessos semelhantes na autenticação;

5.6.3.62. Funcionalidades de Web Application Firewall

5.6.3.63. Deverá ser capaz de identificar e bloquear ataques através de um banco de dados de assinaturas de vírus e reputação IP, atualizado de forma automática;

5.6.3.64. Deve implementar recursos de Sandbox para análise de malware moderno;

5.6.3.65. Deverá implementar recurso de Machine Learning, que permita implementar proteção para um servidor ou grupo de servidores de aplicação web e APIs, de forma automatizada através da análise da utilização da aplicação, fazendo a descoberta da estrutura e padrões de uso, buscando separar o comportamento anormal do abusivo, detectando anomalias e tentativas de ataque;

5.6.3.66. Deve implementar proteção contra a lista de técnicas/ataques listados no OWASP 10 (Open Web Application security Project);

5.6.3.67. Deve implementar recursos embarcados de antivírus para análise de arquivos, detecção e bloqueio de malwares que possam comprometer os servidores possuindo integração com a nuvem do fabricante para obter atualizações, enviar e receber amostras de malware para análise/verificação;

5.6.3.68. Ter a capacidade de criação de assinaturas de ataque customizáveis;

5.6.3.69. Deve implementar recursos de proteção de API (Application Programming Interface) que são implementadas usando XML, JSON API e RESTful API. A solução deve analisar o conteúdo de cada chamada API e aplicar a validação das políticas para proteger contra tráfego malicioso; Ter a capacidade de proteção para ataques do tipo Adobe Flash binary (AMF) protocol;

5.6.3.70. Ter a capacidade de proteção para ataques do tipo Botnet;

5.6.3.71. Ter a capacidade de proteção para ataques do tipo Browser Exploit Against SSL/TLS (BEAST);

5.6.3.72. A solução deverá possuir funcionalidade de proteção positiva contra ataques como acesso por força bruta;

5.6.3.73. Deve suportar detecção a ataques de Clickjacking;

5.6.3.74. Deve suportar detecção a ataques de alteração de cookie;

5.6.3.75. Deve identificar e prevenir ataques do tipo Credit Card Theft;

5.6.3.76. Deve identificar e prevenir ataque Cross Site Request Forgery (CSRF);

5.6.3.77. A solução deve possuir funcionalidade de proteção positiva contra ataques como cross site scripting (XSS);

5.6.3.78. Deve possuir proteção contra ataques de Denial of Service (DoS);

5.6.3.79. Deve possuir a capacidade de proteção para ataques do tipo HTTP header overflow;

5.6.3.80. Deve possuir a capacidade de proteção para ataques do tipo Local File inclusion (FLI);

5.6.3.81. Deve possuir a capacidade de proteção para ataques do tipo Man-in-the-middle (MITM). Deve possuir a capacidade de proteção para ataques do tipo Remote File Inclusion (RFI);

5.6.3.82. Deve possuir a capacidade de proteção para ataques do tipo Server Information Leakage;

5.6.3.83. Deve possuir proteção contra envios de comandos SQL escondidos nas requisições enviadas a bases de dados (SQL Injection);

5.6.3.84. Deve possuir a capacidade de proteção para ataques do tipo Malformed XML;

5.6.3.85. Deve Identificar e prevenir ataques do tipo Low-rate DoS;

5.6.3.86. Deve possuir prevenção contra Slow POST attack;

5.6.3.87. Deve proteger contra ataques Slowloris;

5.6.3.88. Deve possuir a capacidade de proteção para ataques do tipo SYN flood;

5.6.3.89. Deve possuir a capacidade de proteção para ataques do tipo Forms Tampering;

5.6.3.90. A solução deve possuir funcionalidade de proteção positiva contra ataques de manipulação de campo escondido;

5.6.3.91. Deve possuir a capacidade de proteção para ataques do tipo Directory Traversal;

5.6.3.92. Deve possuir a capacidade de proteção do tipo Access Rate Control;

5.6.3.93. Deve possuir a habilidade de configurar proteção do tipo TCP SYN flood-style para prevenção de DoS para qualquer política, através de Syn Cookie e Half Open Threshold;

5.6.3.94. Deve permitir configurar regras de bloqueio a métodos HTTP indesejados;

5.6.3.95. Deve permitir que sejam configuradas regras de limite de upload por tamanho de arquivo;

5.6.3.96. Deve permitir que o administrador bloqueie o tráfego de entrada e/ou tráfego de saída com base nos países, sem a necessidade de gerir manualmente os ranges de endereços IP correspondentes a cada país;

5.6.3.97. Deve suportar a criação de políticas por geolocalização, permitindo que o tráfego de determinado país seja bloqueado;

5.6.3.98. Deve permitir configurar listas negras de bloqueio e listas brancas de confiança, baseadas em endereço IP de origem;

5.6.3.99. Deve permitir a liberação temporária ou definitiva (whitelist) de endereços IP bloqueados por terem originados ataques detectados pela solução;

5.6.3.100. Deve permitir adicionar, automaticamente ou manualmente, em uma lista de bloqueio, os endereços IP de origem, de acordo com a base de IP Reputation;

5.6.3.101. Deve possuir a capacidade de Prevenção ao Vazamento de Informações (DLP), bloqueando o vazamento de informações de cabeçalho HTTP;

5.6.3.102. Deve possuir a funcionalidade de proteger o website contra ações de desfiguração (defacement), com restauração automática e rápida do site caso ocorra à falha;

5.6.3.103. Deve possuir a funcionalidade de antivírus para inspeção de tráfego e arquivos;

5.6.3.104. Deve possuir a capacidade de investigar e analisar todo o tráfego HTTP para atestar se está em conformidade com a respectiva RFC, bloqueando ataques e tráfego em não-conformidade;

5.6.3.105. Deve ser capaz de fazer aceleração de SSL, onde os certificados digitais são instalados na solução e as requisições HTTP são enviadas aos servidores sem criptografia;

5.6.3.106. A solução deve ser capaz de funcionar como Terminador de sessões SSL para a aceleração de tráfego;

5.6.3.107. Deve para SSL/TLS offload suportar no mínimo TLS 1.0, 1.1, 1.2 e 1.3;

5.6.3.108. A solução deve ter a capacidade de armazenar certificados digitais de CA's;

5.6.3.109. A solução deve ser capaz de gerar CSR para ser assinado por uma CA;

5.6.3.110. A solução deve ser capaz de validar os certificados que são válidos e não foram revogados por uma lista de certificados revogados (CRL);

5.6.3.111. A solução deve conter as assinaturas de robôs conhecidos como link checkers, indexadores de web, search engines, spiders e web crawlers que podem ser colocados nos perfis de controle de acesso, bem como resetar tais conexões;

5.6.3.112. A solução deve ter um sistema de reputação de endereços IP públicos conhecidos como fontes de ataques DDoS, botnets, spammers, etc. Tal sistema deve ser atualizado automaticamente;

5.6.3.113. A solução deverá ser capaz de limitar o total de conexões permitidas para cada servidor real de um pool de servidores;

5.6.3.114. A solução deve permitir a customização ou redirecionar solicitações e respostas HTTP no HTTP Host, Request URL HTTP, HTTP Referer, HTTP Body e HTTP Location;

5.6.3.115. A solução deve permitir criar regras definindo a ordem em que as páginas devem ser acessadas para prevenir ataques como cross-site request forgery (CSRF);

5.6.3.116. A solução deve ter a capacidade de definir restrições a métodos HTTP;

5.6.3.117. A solução deve ter a capacidade de proteger contra a detecção de campos ocultos;

5.6.3.118. Deve permitir que sejam criadas assinaturas customizadas de ataques e DLP, através de expressões regulares;

5.6.3.119. A solução deve incluir capacidade de atuar como um scanner de vulnerabilidades ou permitir a integração com scanners de vulnerabilidade de terceiros para diagnóstico e identificação de ameaças nos servidores web, software desatualizado e potenciais buffers overflows;

5.6.3.120. Deve gerar perfil de proteção automaticamente a partir de relatório em formato XML gerado por scanner de vulnerabilidade de terceiros;

5.6.3.121. A solução deve gerar um relatório da análise de vulnerabilidades no formato HTML;

5.6.3.122. A solução deve permitir a exclusão de URLs na análise de vulnerabilidades;

5.6.3.123. Deve ser capaz de fazer compressão de conteúdo HTTP, para reduzir a quantidade de informações enviadas ao cliente;

5.6.3.124. Deve suportar redireção e reescrita de requisições e respostas HTTP;

5.6.3.125. Deve permitir redirecionar requisições HTTP para HTTPS;

5.6.3.126. Deve permitir reescrever a linha URL no cabeçalho de uma requisição HTTP;

5.6.3.127. Deve permitir reescrever o campo "Host:" no cabeçalho de uma requisição HTTP;

5.6.3.128. Deve permitir reescrever o campo "Referer:" no cabeçalho de uma requisição HTTP;

5.6.3.129. Deve permitir redirecionar requisições para outro web site;

5.6.3.130. Permitir enviar resposta HTTP 403 Forbidden para requisições HTTP;

5.6.3.131. Deve permitir reescrever o parâmetro "Location:" no cabeçalho HTTP de uma resposta de redireção HTTP de um servidor web;

5.6.3.132. Deve permitir reescrever o corpo ("body") de uma resposta HTTP de um servidor web;

5.6.3.133. Deve permitir adicionar o campo X-Forwarded-For para identificação do endereço real do cliente quando no modo de proxy reverso;

5.6.3.134. A solução deve suportar regras para definir se as solicitações HTTP serão aceitas com base na URL e a origem do pedido e, se necessário, aplicar uma taxa específica de transferência (rate limit);

5.6.3.135. A solução deve suportar o mecanismo de combinação de controle de acesso e autenticação utilizando mecanismos como HTML Form, Basic e Suporte a SSO, métodos como LDAP e RADIUS para consultas e integração dos usuários da aplicação;

5.6.3.136. Possuir capacidade de caching para aceleração web;

5.6.3.137. Deve permitir ao Administrador a criação de novas assinaturas e/ou alteração de assinaturas já existentes;

5.6.3.138. Deve ser capaz de restringir acesso quando as requisições não tiverem um cabeçalho HTTP específico pré-configurado;

5.6.3.139. Deve ser capaz de limitar o número de usuários/origens simultâneos acessando a mesma conta/sessão/login;

5.6.3.140. Deve ser capaz de criptografar URLs para prevenir acesso forçado e garantir que a estrutura de diretórios interna da aplicação web não seja revelada aos usuários;

5.6.3.141. Deve ser capaz de adicionar múltiplos servidores ADFS em um pool de servidores;

5.6.3.142. Funcionalidades de Balanceamento de Carga

5.6.3.143. A solução deve incluir funcionalidade de balanceamento de carga entre servidores web;

5.6.3.144. Deve possuir a habilidade de configurar portas não-padrão para aplicação web HTTP e HTTPS;

5.6.3.145. Deve possuir a capacidade de balancear/distribuir tráfego e rotear o conteúdo através de vários servidores web;

5.6.3.146. A solução deve permitir criar grupos de servidores (Server Farm / Pool) para distribuir as conexões dos usuários;

5.6.3.147. Deve suportar algoritmo Round Robin para balanceamento de carga de servidores;

5.6.3.148. Deve suportar algoritmo Weighted Round Robin para balanceamento de carga de servidores;

5.6.3.149. Deve suportar algoritmo Least Connections para balanceamento de carga de servidores;

5.6.3.150. A solução deve ser capaz de criar servidores virtuais que definem a interface de rede/bridge e endereço IP por onde o tráfego destinado ao Server Pool é recebido;

5.6.3.151. Os servidores virtuais devem entregar o tráfego à um único servidor web e também possuir a opção de distribuir as sessões/conexões entre os servidores web do Server Pool;

5.6.3.152. Deve ser possível especificar o número máximo de conexões TCP simultâneas para um determinado servidor membro do Server Pool;

5.6.3.153. Deve permitir teste de disponibilidade de servidor web através do método TCP;

5.6.3.154. Deve permitir teste de disponibilidade de servidor web através do método ICMP ECHO_REQUEST (ping);

5.6.3.155. Deve permitir teste de disponibilidade de servidor web através do método TCP Half Open;

5.6.3.156. Deve permitir teste de disponibilidade de servidor web através do método TCP SSL;

5.6.3.157. Deve permitir teste de disponibilidade de servidor web através do método HTTP;

5.6.3.158. Deve permitir teste de disponibilidade de servidor web através do método HTTPS;

5.6.3.159. Nos testes de disponibilidade HTTP e HTTPS, permitir indicar a URL exata a ser testada;

5.6.3.160. Nos testes de disponibilidade HTTP e HTTPS, permitir escolher entre os métodos HEAD, GET e POST;

5.6.3.161. Nos testes de disponibilidade HTTP e HTTPS, permitir indicar o nome do campo HTTP "host" a ser testado;

5.6.3.162. Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de “Host”;

5.6.3.163. Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de “URL”;

5.6.3.164. Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de “Parâmetro HTTP”;

5.6.3.165. Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de “Referer”;

5.6.3.166. Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de “Endereço IP de Origem”;

5.6.3.167. Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de “Cabeçalho”;

5.6.3.168. Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de “Cookie”;

5.6.3.169. Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de “Valor de campo do Certificado X509”;

5.6.3.170. Deve implementar Cache de Conteúdo para HTTP, permitindo que objetos sejam armazenados e requisições HTTP sejam respondidas diretamente pela solução;

5.6.3.171. A solução deve ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência por endereço IP de origem;

5.6.3.172. A solução deve ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência analisando parâmetros do header HTTP;

5.6.3.173. A solução deve ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência analisando a URL acessada;

5.6.3.174. A solução deve ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência por cookie – método cookie insert e cookie rewrite;

5.6.3.175. A solução deve ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência por embedded cookie (cookie original mais porção randômica);

5.6.3.176. A solução deve ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência baseada em Reescrita de Cookie;

5.6.3.177. A solução deve ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência baseada em Cookie Persistente;

5.6.3.178. A solução ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência baseada em ASP Session ID;

5.6.3.179. A solução deve ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência baseada em PHP Session ID;

5.6.3.180. A solução deve ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência baseada em JSP Session ID;

5.6.3.181. A solução deve ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência por sessão SSL;

5.6.3.182. A solução deve ser capaz de enviar código de erro 503 caso o helth-check dos servidores estiver desabilitado e/ou o servidor/serviço de retaguarda não estiver responsivo;

5.6.3.183. Deve suportar FWMARK (marcação de tráfego).

6 - DAS OBRIGAÇÕES E DEVERES DAS PARTES

6.1. A CONTRATANTE obriga-se a:

a) **designar** equipe de servidores do Órgão para acompanhar e fiscalizar a execução do objeto da contratação, nos termos fixados no art. 67 da Lei 8.666/93;

b) **exigir**, por intermédio da Fiscalização, o cumprimento integral das obrigações assumidas pela CONTRATADA, observadas rigorosamente as condições contidas neste Termo de Referência;

c) **prover** condições que possibilitem e facilitem a execução dos serviços objeto deste Termo;

d) **prestar** as informações e os esclarecimentos necessários ao bom andamento das atividades;

e) **receber, analisar e atestar** as notas fiscais/faturas que são de responsabilidade da CONTRATADA, nos termos fixados neste Termo de Referência;

f) **intervir**, cautelar e diretamente, na execução do contrato para fins de evitar possíveis danos ao interesse público primário, nas situações e nos limites previstos na legislação vigente;

g) **aplicar**, mediante processo administrativo, eventuais **sanções administrativas** nos casos de ilícitos ou inadimplementos contratuais por parte da CONTRATADA (e seus prepostos, responsáveis e empregados), conforme fixado neste Termo de Referência e na legislação vigente;

h) **exigir**, durante toda a vigência do contrato, a **manutenção das condições de habilitação** em compatibilidade com as regras exigidas na licitação;

i) **alterar**, mediante aditamento, o **escopo do objeto** definido neste Termo, sempre no sentido de **melhor atender ao interesse público primário** e observados os limites legalmente fixados, mediante prévio pronunciamento da Fiscalização;

j) **assegurar** o acesso de pessoal autorizado pela CONTRATADA, desde que devidamente identificados, para a execução do objeto contratado, tomando todas as providências necessárias;

k) **controlar** as ligações realizadas, documentando as ocorrências havidas;

l) **registrar** eventuais ocorrências e anormalidades na prestação dos serviços;

m) **observar** as demais obrigações decorrentes da legislação correlata;

n) **cumprir** e fazer cumprir todas as demais disposições contidas neste Termo de Referência.

6.2 – A CONTRATADA obriga-se a:

a) **credenciar** por escrito, junto ao CONTRATANTE, um preposto idôneo com poderes de decisão para representar a empresa, principalmente no tocante à eficiência e agilidade da execução dos serviços objeto deste Termo de Referência;

b) **executar** os serviços contratados em estrita observância às especificações, condições, parâmetros e prazos definidos neste Termo de Referência, bem como observando as exigências e as solicitações e determinações da Fiscalização;

c) **fornecer** os softwares, equipamentos e acessórios necessários à execução dos serviços previstos neste Termo de Referência;

d) **responsabilizar-se** por todos os encargos comerciais, trabalhistas, fiscais e sociais decorrentes da contratação;

e) **responsabilizar-se** pela quitação e/ou cumprimento de eventuais sanções administrativas aplicadas pela CONTRATANTE em decorrência de ilícitos ou inadimplementos contratuais;

f) **cumprir** todos os prazos expressamente fixados neste Termo de Referência, bem com aqueles fixados diretamente pela Fiscalização;

g) **reparar ou corrigir**, às suas expensas, no total ou em parte, os serviços que compõem o escopo do objeto da Contratação em que se verificarem vícios, defeitos ou incorreções;

h) **responsabilizar-se** por quaisquer danos causados à CONTRATANTE ou a terceiros ocorridos durante a execução do objeto e em decorrência dela;

i) **apresentar** a documentação necessária à liquidação e pagamento da despesa para fins atestação da Fiscalização, observadas as regras fixadas neste Termo de Referência e na legislação vigente;

j) **manter-se**, durante a execução do Contrato, em compatibilidade com as condições de habilitação e qualificação exigidas na licitação;

k) **responder** por quaisquer interferências de estranhos nos acessos em serviço, bem como zelar pela integridade das comunicações;

l) **implantar**, de forma adequada, a supervisão permanente dos serviços, de modo a obter uma operação correta e eficaz;

m) **comunicar** ao CONTRATANTE, por escrito ou através de e-mail, qualquer anormalidade nos serviços e prestar os esclarecimentos julgados necessários;

n) **em nenhuma hipótese**, veicular publicidade ou qualquer outra informação acerca da prestação dos serviços do Contrato, sem prévia autorização do CONTRATANTE;

o) **responsabilizar-se** pelos ônus resultantes de quaisquer ações, demandas, custos e despesas decorrentes de danos, ocorridos por culpa sua ou de qualquer de seus empregados e prepostos obrigando-se, outrossim, por quaisquer responsabilidades decorrentes de ações judiciais movidas por terceiros, que lhe venham a ser exigidas por força da Lei, ligadas ao cumprimento do Contrato;

p) **observar** as demais obrigações decorrentes da legislação correlata;

q) **cumprir** outras exigências contidas neste Termo de Referência, bem como solicitações e determinações da Fiscalização;

r) **executar** outras atividades e procedimentos necessários ao fiel cumprimento das obrigações contratuais nos termos fixados neste Termo de Referência.

7 - DA DINÂMICA DE EXECUÇÃO DOS SERVIÇOS

7.1. Da execução dos serviços:

7.1.1. Por tratar-se de prestação de serviço de locação, objeto da futura contratação, deverá ser realizado diretamente pela CONTRATADA de modo a cumprir o escopo contratual nas condições pactuadas, observadas rigorosamente as especificações técnicas contidas neste Termo de Referência, a legislação vigente e as boas técnicas de cada área de especialidade.

7.2. Do prazo de execução dos serviços

7.2.1. Os serviços serão executados de forma continuada e o cronograma de execução será definido em comum acordo com a empresa CONTRATADA.

8 – DO PRAZO DE VIGÊNCIA DO CONTRATO

8.1. O presente Contrato terá vigência de 12 (doze) meses, contados a partir da data de sua assinatura, e poderá ser prorrogado por iguais e sucessivos períodos com base no inciso II, art. 57 da Lei Federal 8.666/93.

9 - PREVISÃO ORÇAMENTÁRIA

9.1. A execução do presente contrato será custeada com recursos financeiros oriundos do Orçamento desta Casa Legislativa, na classificação funcional programática 01101.01122.5046.4216, no elemento de despesa 33903900.100.

10 - DO PAGAMENTO

10.1. Os pagamentos, mediante a emissão de Nota Fiscal com código de barras, serão realizados desde que a **CONTRATADA** efetue a cobrança de forma a permitir o cumprimento das exigências legais, principalmente no que se refere às retenções tributárias.

10.2. O fiscal do contrato atestará a nota fiscal, com ou sem ressalvas, no prazo de até 10 (dez) dias úteis a contar do recebimento da mesma.

10.3. No caso de a nota fiscal ser atestada com ressalva de que durante a entrega ou execução dos serviços de instalação ocorreu fato passível de aplicação de penalidades contratuais; a CONTRATADA, após a ciência do fato, terá o prazo de 20 (vinte) dias úteis para sanar o ocorrido, devendo o gestor, decorrido este período, encaminhar o processo à Administração para as medidas cabíveis.

10.4. O prazo de pagamento ocorrerá no prazo máximo de 30 (trinta) dias após o recebimento definitivo de cada solicitação, contados do aceite das Faturas / Notas Fiscais.

10.5. Os pagamentos somente serão efetuados após a comprovação, pela Contratada, de que se encontra regular com suas obrigações, mediante a apresentação das Certidões Negativas de Débito.

10.6. Ocorrendo erro no documento da cobrança, este será devolvido e o pagamento será sustado, para que a contratada tome as medidas necessárias, passando o prazo para o pagamento a ser contado a partir da data da reapresentação do mesmo.

10.7. Caso se constate erro ou irregularidade na Nota Fiscal, o Órgão, ao seu critério, poderá devolvê-la, para as devidas correções, ou aceitá-la.

10.8. Na hipótese de devolução, a Nota Fiscal será considerada como não apresentada, para fins de atendimento das condições contratuais.

10.9. Na pendência de liquidação da obrigação financeira, em virtude de penalidade ou inadimplência contratual, o valor será descontado da fatura ou créditos existentes em favor do fornecedor.

10.10 O órgão não pagará, sem que tenha autorização prévia e formal, nenhum compromisso que lhe venha a ser cobrado diretamente por terceiros, seja ou não instituições financeiras.

10.11. Os eventuais encargos financeiros, processuais e outros, decorrentes da inobservância de prazo de pagamento pela Contratada, serão de sua exclusiva responsabilidade.

10.12. A Administração efetuará retenção na fonte, dos tributos e contribuições sobre todos os pagamentos devidos à Contratada.

11 - FISCALIZAÇÃO DO CONTRATO

11.1. Para garantir maior racionalização e objetividade à execução do contrato de prestação do serviço, a **ASSEMBLEIA LEGISLATIVA DO ESTADO DA PARAÍBA** e a CONTRATADA deverão indicar, oficialmente, no ato da assinatura do contrato, profissionais que os representarão, passando a atuar como Fiscal e Preposto, respectivamente.

11.2. Os aludidos representantes do contrato ficarão responsáveis pelas atividades de planejamento, coordenação e controle da execução de todo o projeto, além do acompanhamento do cumprimento dos prazos e metas estabelecidos, além da aprovação das faturas relativas à prestação dos serviços.

Ao Fiscal do Contrato nomeado pelo órgão CONTRATANTE caberá, entre outras atribuições:

a) Zelar para que as atividades a cargo do órgão CONTRATANTE sejam cumpridas dentro dos prazos estabelecidos;
b) Acompanhar execução dos serviços a cargo da CONTRATADA, permitindo, se necessário, sempre que informado previamente, o acesso dos técnicos às instalações das unidades da CONTRATANTE, de modo a possibilitar a execução das implantações, ampliações e manutenções preventivas, a fim de fazer cumprir o objeto licitado;
c) Zelar para que os serviços de manutenções corretivas sejam executados dentro dos prazos contratuais, com os respectivos registros dos códigos de abertura dos chamados, que garantirão o acesso dos técnicos às instalações

das unidades do órgão CONTRATANTE;
d) Zelar para que os profissionais alocados pela CONTRATADA para prestação dos serviços só tenham acesso às dependências das unidades do órgão CONTRATANTE mediante apresentação de cartões de identificação profissional com fotografia e número de identidade;
e) Manter registro das atividades relacionadas ao desenvolvimento do contrato;
f) Agendar reuniões periódicas com a CONTRATADA para avaliação dos serviços prestados, recomendar alternativas de soluções para os problemas detectados, apontando eventuais deficiências verificadas na execução dos serviços e solicitando imediata correção, sem prejuízo da aplicação das penalidades previstas em contrato;
g) Conferir pormenorizadamente os valores cobrados nas faturas emitidas pela CONTRATADA.

11.3. À CONTRATADA, através do Preposto do contrato, por ela nomeado, caberá, entre outras responsabilidades:

a) Assegurar o sigilo sobre as informações relativas ao órgão CONTRATANTE;
b) Zelar para que as atividades a cargo da CONTRATADA sejam cumpridas dentro dos prazos estabelecidos;
c) Assegurar a capacitação necessária das equipes responsáveis pela realização dos trabalhos;
d) Acompanhar a execução dos serviços, solicitando, quando necessário, o acesso de seus técnicos às instalações das unidades do órgão CONTRATANTE, de modo a possibilitar a execução das implantações, ampliações e manutenções preventivas, a fim de fazer cumprir o objeto licitado;
e) Zelar para que os serviços de manutenção/reparo corretivos sejam executados dentro dos prazos contratuais, mediante registros dos códigos de abertura dos chamados, que garantirão o acesso dos técnicos às instalações das unidades do órgão CONTRATANTE;
f) Zelar pela permanente manutenção dos equipamentos que compõem o objeto do contrato, garantindo boas condições de funcionamento, providenciando todos os ajustes, reparos e substituições de peças que se façam necessárias;
g) Garantir que nas substituições de equipamentos em operação, em caso de defeitos, os novos equipamentos operem com qualidade igual ou superior, pelo tempo necessário até a devolução do original, excetuando-se os casos previstos na cláusula anterior;
h) Zelar para que a remoção de quaisquer equipamentos em operação, quando necessária, seja comunicada previamente ao Fiscal do Contrato nomeado pelo órgão CONTRATANTE, bem como os motivos da retirada, a previsão de retorno e a devolução para os locais de origem;
i) Garantir que todos os profissionais alocados para prestação de serviço nas dependências do órgão CONTRATANTE apresentem cartões de identificação profissional com fotografia e número de identidade, para que tenham acesso controlado;
j) Providenciar imediata substituição, ante a expressa manifestação escrita do Fiscal do Contrato nomeado pelo órgão CONTRATANTE, de quaisquer de seus profissionais encarregados da execução dos serviços, que não corresponderem aos princípios éticos e morais nas suas dependências;
k) Garantir que todas as atividades sejam realizadas dentro dos padrões de qualidade, segurança e higiene, observando os requisitos da medicina do trabalho e prevenção contra incêndios;
l) Manter registro das atividades relacionadas ao desenvolvimento do contrato;
m) Participar de reuniões periódicas com o CONTRATANTE para avaliação dos serviços prestados, apresentando soluções para os problemas detectados, adotando providências no sentido de superar eventuais deficiências verificadas na execução dos serviços.

12 - FUNDAMENTO LEGAL

12.1. O procedimento licitatório a ser adotado obedecerá, integralmente, ao que estabelece:

a) A Constituição Federal (artigo 37, XXI);
b) A Lei Federal nº 8.666/93, e suas alterações posteriores;
c) A Lei Federal nº 10.520/02;
d) A Lei Complementar 123/2006;
e) A Resolução nº 1.219/2007;
f) As Demais legislações pertinentes.

13 – QUALIFICAÇÃO TÉCNICA EXIGIDA DO(S) CONTRATADO(S)

13.1. Para o LOTE 01:

a) Apresentar documento(s) expedido(s) pela ANATEL – Agência Nacional de Telecomunicações, dentro do prazo de validade, comprovando ser empresa constante no rol das autorizadas por esta Agência Reguladora para prestar Serviço de Comunicação Multimídia ou documento comprovando seu registro como operadora dispensada da referida licença. As licitantes podem apresentar os extratos da publicação no Diário Oficial do Contrato de Concessão, do Termo de Autorização ou equivalente;
b) Apresentar atestado com pelo menos 01 link de 1Gbps e 01 de 500 Mbps com solução DDoS;

13.2. Para o LOTE 02:

a) Apresentar atestado de capacidade técnica com fornecimento ou serviço, de no mínimo 30%, de solução de segurança deste termo de referência;
b) A empresa deverá apresentar, pelo menos, 01 (um) profissional qualificado com certificação técnica oficial do fabricante dos equipamentos ofertados, capaz de prestar o serviço de implantação e customização dos equipamentos e softwares ofertados.

14 - DISPOSIÇÕES GERAIS

14.1. Poderão apresentar proposta todas e quaisquer pessoas jurídicas, legalmente constituídas e estabelecidas, que estejam capacitadas a atender ao seu objeto e demais requisitos e habilitadas pelo poder concedente nos termos da legislação em vigor.

ANEXO I AO TR – PLANILHA DE QUANTITATIVOS

LOTE	ITEM	Descrição serviço	Qtd	Unidade
01	01	Assinatura link INTERNET 1Gbps Assinatura para serviço de segurança e mitigação contra-ataques ANTI-DDOS (por link Internet).	02	Assinatura
	02	Assinatura link INTERNET 500Mbps Assinatura para serviço de segurança e mitigação contra-ataques ANTI-DDOS (por link Internet).	02	Assinatura
02	01	Solução de Segurança de Redes NGFW **TIPO 1** com 60 meses de atualização de firmware, atualização automática de bases de dados, suporte e garantia do fabricante.	0 2	Assinatura
	02	Solução de Segurança de Redes NGFW **TIPO 2** com 60 meses de atualização de firmware, atualização automática de bases de dados, suporte e garantia do fabricante.	02	Assinatura
	03	Serviços de solução de controle de acesso a rede (NAC) com 60 meses de atualização de firmware, atualização automática de bases de dados, suporte e garantia do fabricante.	01	Assinatura
	04	Solução de segurança de aplicações WEB e API - Firewall de Aplicação (WAF) com 60 meses de atualização de firmware, atualização automática de bases de dados, suporte e garantia do fabricante.	01	Assinatura

ANEXO II AO TR – LISTA DE LOCALIDADES E ENDEREÇOS

Os serviços serão executados nas dependências da Sala de Telecomunicações do Centro Administrativo e Operacional da Assembleia Legislativa da Paraíba, situado à Praça João Pessoa, s/n – Centro, na Creche Pré-Escola Ângela Maria Meira de Carvalho e nos anexos da desta Casa Legislativa.

1. Praça João Pessoa, SN - Centro, João Pessoa - PB, 58010-100;
2. Av. Dom Pedro I, 445 - Tambiá, João Pessoa - PB, 58013;
3. Praça Vidal de Negreiros, 276 - Centro, João Pessoa - PB, 58010-810;
4. Rua Des. Souto Maior, 77 - Centro, João Pessoa - PB, 58013-190.

ESTADO DA PARAÍBA
ASSEMBLÉIA LEGISLATIVA
COMISSÃO PERMANENTE DE LICITAÇÃO

PREGÃO PRESENCIAL Nº 28/2023

ANEXO II

MODELO DE PROPOSTA DE PREÇOS

À ASSEMBLEIA LEGISLATIVA DO ESTADO DA PARAÍBA

Proposta para atendimento do objeto destinado a Assembleia Legislativa da Paraíba, em conformidade com o Edital de Pregão Presencial **nº 28/2023**, autorizado pelo Processo Administrativo **nº 3244/2023.**

Para tanto, oferecemos a este Poder Legislativo o preço para o item abaixo, observadas as exigências e especificações de que tratam o **ANEXO I – TERMO DE REFERÊNCIA.**

LOTE	ITEM	Descrição serviço	Qtd	Unidade	Valor Unitário	Valor Total Mensal	Valor Total Anual
01	01	Assinatura link INTERNET 1Gbps Assinatura para serviço de segurança e mitigação contra-ataques ANTI-DDOS (por link Internet).	02	Assinatura			
	02	Assinatura link INTERNET 500Mbps Assinatura para serviço de segurança e mitigação contra-ataques ANTI-DDOS (por link Internet).	02	Assinatura			
	VALORES TOTAIS MENSAL E ANUAL DO LOTE I						
02	01	Solução de Segurança de Redes NGFW **TIPO 1** com 60 meses de atualização de firmware, atualização automática de bases de dados, suporte e garantia do fabricante.	0 2	Assinatura			
	02	Solução de Segurança de Redes NGFW **TIPO 2** com 60 meses de atualização de firmware, atualização automática de bases de dados, suporte e garantia do fabricante.	02	Assinatura			
	03	Serviços de solução de controle de acesso a rede (NAC) com 60 meses de atualização de firmware, atualização automática de bases de dados, suporte e garantia do fabricante.	01	Assinatura			
	04	Solução de segurança de aplicações WEB e API - Firewall de Aplicação (WAF) com 60 meses de atualização de firmware, atualização automática de bases de dados, suporte e garantia do fabricante.	01	Assinatura			
	VALORES TOTAIS MENSAL E ANUAL DO LOTE II						
VALORES TOTAIS MENSAL E ANUAL DOS LOTES I + II							

A validade da presente proposta é de 60 (sessenta) dias corridos, contados da sua abertura, observado o disposto no *caput* e parágrafo único do art. 110 da Lei no 8.666/93.

Os preços ofertados já incluem a entrega e retirada dos itens no local determinado.

Informamos, por oportuno, que no preço estão incluídos todos os custos diretos e indiretos para o perfeito fornecimento do objeto, inclusive os encargos da legislação social, trabalhista, previdenciária, englobando tudo o que for necessário para a execução total e completa do objeto licitado, conforme especificações constantes no Edital e seus Anexos.

Os dados da nossa empresa são:

a) Razão Social:

b) CNPJ:

c) Inscrição Estadual/Municipal:

d) Endereço:

e) Fone/e-mail:

f) Cidade/Estado/CEP:

g) Banco/Agência/Conta Corrente:

Declaramos, para todos os fins, que o fornecimento do objeto se dará de acordo com as especificações definidas nesta proposta e respeitando o estabelecido no Edital e seus Anexos.

João Pessoa, ____ de _____ de 2023.

_____
Assinatura e numero da identidade e/ou CPF do representante legal da empresa

ANEXO III

DECLARAÇÃO DE ATENDIMENTO DOS REQUISITOS DE HABILITAÇÃO

A Empresa (nome da Empresa), devidamente inscrita no CNPJ /MF n.º_____, sediada na (endereço completo)_____e e-mail_____; neste ato representada por seu sócio/gerente, o Sr._____, brasileiro, (estado civil), portador da Carteira de Identidade nº_____, inscrito no Cadastro de Pessoas Físicas (CPF) sob o nº_____, com poderes estabelecidos no ato da investidura (atos constitutivos da pessoa jurídica, ata de eleição do outorgante, etc.) conforme cópia em anexo, no uso de suas atribuições legais, declara, sob as penas previstas no subitem 3.3 deste Edital e demais legislações, que preenche todas as condições de qualificação técnica, jurídica e econômico-financeira para a participação no certame, bem como, expressa total aceitação de todas as normas e condições estabelecidas no Pregão Presencial **nº 28/2023**, autorizado pelo processo administrativo **nº 3244/2023.**

Por ser expressa manifestação da verdade, firmo a presente.

(Local), _____de_____de 2023.

_____
Assinatura e número da identidade e/ou CPF do representante legal da empresa

ESTADO DA PARAÍBA
ASSEMBLÉIA LEGISLATIVA
COMISSÃO PERMANENTE DE LICITAÇÃO

PREGÃO PRESENCIAL N° 28/2023

ANEXO IV

DECLARAÇÃO DE QUE NÃO EMPREGA MENOR

Declaro que não há no quadro de pessoal desta Empresa, empregado(s) com menos de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre e, de 16 (dezesseis) anos, em qualquer trabalho, salvo na condição de aprendiz, a partir de 14 (quatorze) anos, nos termos do Inciso XXXIII do art. 7°, da Constituição Federal e art. 27, V, da Lei n.º 8.666, de 21 de Junho de 1.993, sob a nova redação da Lei n.° 9.854, de 27 de Outubro de 1.999.

João Pessoa,_____de_____de 2023.

_____
Assinatura e número da identidade e/ou CPF do representante legal da empresa

ESTADO DA PARAÍBA
ASSEMBLÉIA LEGISLATIVA
COMISSÃO PERMANENTE DE LICITAÇÃO

PREGÃO PRESENCIAL N° 28/2023

ANEXO V

DECLARAÇÃO DE COMPROMISSO

(FATOS SUPERVENIENTES)

A Empresa (nome da Empresa), devidamente inscrita no CNPJ /MF n.º_____, sediada na (endereço completo)_____e email _____, neste ato representada por seu sócio/gerente, o Sr._____, brasileiro, (estado civil), portador da Carteira de Identidade nº_____, inscrito no Cadastro de Pessoas Físicas (CPF/MF) sob o nº _____, no uso de suas atribuições legais, comprometendo-se nos termos da legislação reguladora da matéria, a informar a qualquer tempo, sob pena das penalidades cabíveis, a existência de fatos supervenientes impeditivos à habilitação, decorrente do **Pregão Presencial nº 28/2023**, autorizado pelo **Processo administrativo nº 3244/2023.**

João Pessoa,_____de_____de 2023.

_____
Assinatura e numero da identidade e/ou CPF do representante legal da empresa

ESTADO DA PARAÍBA
ASSEMBLÉIA LEGISLATIVA
COMISSÃO PERMANENTE DE LICITAÇÃO

PREGÃO PRESENCIAL N° 28/2023

ANEXO VI

CARTA DE CREDENCIAMENTO

Pela presente, **(RAZÃO SOCIAL, CNPJ, ENDEREÇO COMPLETO COM CEP)**, representada neste ato pelo Sr. **(RESPONSÁVEL DA LICITANTE, ELENCADO NO CONTRATO SOCIAL OU DOCUMENTO EQUIVALENTE, PARA DESIGNAR PROCURADOR)**, nomeia seu bastante PROCURADOR o Sr.**(NOME COMPLETO, DOCUMENTO DE IDENTIFICAÇÃO, CPF)**, residente e domiciliado **(ENDEREÇO COMPLETO COM CEP)**, para representar a referida Empresa no procedimento licitatório – **(NÚMERO DO PREGÃO)** - podendo para tanto FORMULAR LANCES VERBAIS, FIRMAR DECLARAÇÕES DE VONTADE, MANIFESTAR INTERESSE DE RECORRER, RENUNCIAR, SUPRIR INCORREÇÕES FORMAIS, ASSINAR ATAS E CONTRATOS, ENFIM, DESEMPENHAR TODOS OS ATOS NECESSÁRIOS AO FIEL DESEMPENHO DO PRESENTE MANDATO.

João Pessoa,_____de_____de 2023.

_____
Assinatura e numero da identidade e/ou CPF do representante legal da empresa

ESTADO DA PARAÍBA
ASSEMBLÉIA LEGISLATIVA
COMISSÃO PERMANENTE DE LICITAÇÃO

PREGÃO PRESENCIAL Nº 28/2023

ANEXO VII

MINUTA DE CONTRATO

CONTRATO Nº__/2023 DE PRESTAÇÃO DE SERVIÇOS PRESTAÇÃO DE SERVIÇOS, QUE ENTRE SI CELEBRAM A ASSEMBLÉIA LEGISLATIVA DA PARAÍBA E A EMPRESA _____.

A **ASSEMBLEIA LEGISLATIVA DO ESTADO DA PARAÍBA** com sede na Praça João Pessoa s/n, Centro - João Pessoa/PB, inscrita no CNPJ/MF n° 09.283.912/0001-92, neste ato representada pelo seu Diretor Geral**, Bruno Mouzinho Regis**, brasileiro, portador do RG nº 2.480.948 SSP/PB e CPF nº 034.331.954-39, residente e domiciliado nesta Capital, aqui denominada **Contratante** e do outro lado na qualidade de **Contratada**, a Firma **.....**, inscrita no CNPJ nº ....., estabelecida à ....., representada neste ato pelo Senhor..... , brasileiro, portador do RG nº ..... e CPF nº....., resolvem celebrar por força do presente instrumento, e de conformidade com o disposto na Lei Federal nº 8.666/93 e alterações posteriores, contratação de empresa especializada no ramo para o fornecimento de serviços para formação de rede de dados através de links IP de Internet terrestres, serviço de segurança e mitigação contra ataques ANTI-DDOS, fornecimento de serviços de segurança de perímetro (controle de Regras de Segurança, Firewall, IPS/IDS, Antivírus, Controle de Conteúdo Web, Controle de Acesso à Aplicações, Emissão de Relatórios Periódicos e Segurança Pró-ativa); Fornecimento de solução SD-WAN, controle de acesso de rede (NAC) e segurança de aplicações WEB e API – WAF, mediante as seguintes cláusulas e condições e de acordo com o Processo Administrativo nº **3244/2023,** e o que consta no procedimento licitatório na modalidade **Pregão Presencial nº 28/2023.**

CLÁUSULA PRIMEIRA - DO OBJETO

O objeto do presente Istrumento Contratual é a contratação de pessoa jurídica para o fornecimento de serviços para formação de rede de dados através de links IP de Internet terrestres, serviço de segurança e mitigação contra ataques ANTI-DDOS, fornecimento de serviços de segurança de perímetro (controle de Regras de Segurança, Firewall, IPS/IDS, Antivírus, Controle de Conteúdo Web, Controle de Acesso à Aplicações, Emissão de Relatórios Periódicos e Segurança Pró-ativa); Fornecimento de solução SD-WAN, controle de acesso de rede (NAC) e segurança de aplicações WEB e API – WAF, para atender as necessidades deste Poder Legislativo, pelo período de 12 (doze) meses, conforme especificações abaixo:

LOTE	ITEM	Descrição serviço	Qtd	Unidade	Valor Unitário	Valor Total Mensal	Valor Total Anual
01	01	Assinatura link INTERNET 1Gbps Assinatura para serviço de segurança e mitigação contra-ataques ANTI-DDOS (por link Internet).	02	Assinatura			
	02	Assinatura link INTERNET 500Mbps Assinatura para serviço de segurança e mitigação contra-ataques ANTI-DDOS (por link Internet).	02	Assinatura			
	VALORES TOTAIS MENSAL E ANUAL DO LOTE I						

02	01	Solução de Segurança de Redes NGFW **TIPO 1** com 60 meses de atualização de firmware, atualização automática de bases de dados, suporte e garantia do fabricante.	0 2	Assinatura			
	02	Solução de Segurança de Redes NGFW **TIPO 2** com 60 meses de atualização de firmware, atualização automática de bases de dados, suporte e garantia do fabricante.	02	Assinatura			
	03	Serviços de solução de controle de acesso a rede (NAC) com 60 meses de atualização de firmware, atualização automática de bases de dados, suporte e garantia do fabricante.	01	Assinatura			
	04	Solução de segurança de aplicações WEB e API - Firewall de Aplicação (WAF) com 60 meses de atualização de firmware, atualização automática de bases de dados, suporte e garantia do fabricante.	01	Assinatura			
	VALORES TOTAIS MENSAL E ANUAL DO LOTE II						
VALORES TOTAIS MENSAL E ANUAL DOS LOTES I + II							

CLÁUSULA SEGUNDA - DA DOTAÇÃO ORÇAMENTÁRIA

A execução do presente Contrato será custeada com recursos financeiros oriundos do Orçamento desta Casa Legislativa, na classificação funcional programática 01101.01122.5046.4216, no elemento de despesa 33903900.100.

CLÁUSULA TERCEIRA - DOS PREÇOS

A Contratante pagará à Contratada o valor mensal de R$_____(_____), pelos serviços constantes na Cláusula Primeira do presente instrumento contratual.

Parágrafo Primeiro - Estão incluídos nos preços todos os impostos, taxas, transporte, leis sociais e demais encargos que incidam sobre a execução total do objeto deste Contrato.

CLÁUSULA QUARTA - DA FORMA DE PAGAMENTO

Parágrafo Primeiro – Os pagamentos, mediante a emissão de Nota Fiscal com código de barras, serão realizados desde que a **CONTRATADA** efetue a cobrança de forma a permitir o cumprimento das exigências legais, principalmente no que se refere às retenções tributárias.

Parágrafo Segundo – O fiscal do contrato atestará a nota fiscal, com ou sem ressalvas, no prazo de até 10 (dez) dias úteis a contar do recebimento da mesma.

Parágrafo Terceiro – No caso de a nota fiscal ser atestada com ressalva de que durante a entrega ou execução dos serviços de instalação ocorreu fato passível de aplicação de penalidades contratuais; a CONTRATADA, após a ciência do fato, terá o prazo de 20 (vinte) dias úteis para sanar o ocorrido, devendo o gestor, decorrido este

período, encaminhar o processo à Administração para as medidas cabíveis.

Parágrafo Quarto – O prazo de pagamento ocorrerá no prazo máximo de 30 (trinta) dias após o recebimento definitivo de cada solicitação, contados do aceite das Faturas / Notas Fiscais.

Parágrafo Quinto – Os pagamentos somente serão efetuados após a comprovação, pela Contratada, de que se encontra regular com suas obrigações, mediante a apresentação das Certidões Negativas de Débito.

Parágrafo Sexto – Ocorrendo erro no documento da cobrança, este será devolvido e o pagamento será sustado, para que a contratada tome as medidas necessárias, passando o prazo para o pagamento a ser contado a partir da data da reapresentação do mesmo.

Parágrafo Sétimo – Caso se constate erro ou irregularidade na Nota Fiscal, o Órgão, ao seu critério, poderá devolvê-la, para as devidas correções, ou aceitá-la.

Parágrafo Oitavo – Na hipótese de devolução, a Nota Fiscal será considerada como não apresentada, para fins de atendimento das condições contratuais.

Parágrafo Nono – Na pendência de liquidação da obrigação financeira, em virtude de penalidade ou inadimplência contratual, o valor será descontado da fatura ou créditos existentes em favor do fornecedor.

Parágrafo Décimo – O órgão não pagará, sem que tenha autorização prévia e formal, nenhum compromisso que lhe venha a ser cobrado diretamente por terceiros, seja ou não instituições financeiras.

Parágrafo Décimo Primeiro – Os eventuais encargos financeiros, processuais e outros, decorrentes da inobservância de prazo de pagamento pela Contratada, serão de sua exclusiva responsabilidade.

Parágrafo Décimo Segundo – A Administração efetuará retenção na fonte, dos tributos e contribuições sobre todos os pagamentos devidos à Contratada.

Parágrafo Décimo Terceiro - Nos casos de eventuais atrasos de pagamento, desde que a CONTRATADA não tenha concorrido, de forma alguma, 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 pagamento e do efetivo pagamento;
VP = Valor da parcela a ser paga;
I = Índice de compensação financeira = 0,00016438, assim apurado:
I = (TX)
I = (6 / 100) I = 0,00016438
365 TX = Percentual da taxa anual = 6%

Parágrafo Décimo Quarto - O pagamento será processado através do Banco _____, Agência _____, Conta Corrente _____.

CLÁUSULA QUINTA – DA DINÂMICA DE EXECUÇÃO DOS SERVIÇOS

Parágrafo Primeiro – Da execução dos serviços:

Por tratar-se de prestação de serviço, o objeto da futura contratação deverá ser realizado diretamente pela

CONTRATADA de modo a cumprir o escopo contratual nas condições pactuadas, observadas rigorosamente as especificações técnicas contidas neste Termo de Referência, a legislação vigente e as boas técnicas de cada área de especialidade.

Parágrafo Segundo – Do prazo de execução dos serviços:

Os serviços serão executados de forma continuada e o cronograma de execução será definido em comum acordo com a empresa CONTRATADA.

CLÁUSULA SEXTA - OBRIGAÇÕES E RESPONSABILIDADES DA CONTRATANTE

A CONTRATANTE obriga-se a:

a) **designar** equipe de servidores do Órgão para acompanhar e fiscalizar a execução do objeto da contratação, nos termos fixados no art. 67 da Lei 8.666/93;

b) **exigir**, por intermédio da Fiscalização, o cumprimento integral das obrigações assumidas pela CONTRATADA, observadas rigorosamente as condições contidas neste Termo de Referência;

c) **prover** condições que possibilitem e facilitem a execução dos serviços objeto deste Termo;

d) **prestar** as informações e os esclarecimentos necessários ao bom andamento das atividades;

e) **receber, analisar e atestar** as notas fiscais/faturas que são de responsabilidade da CONTRATADA, nos termos fixados neste Termo de Referência;

f) **intervir**, cautelar e diretamente, na execução do contrato para fins de evitar possíveis danos ao interesse público primário, nas situações e nos limites previstos na legislação vigente;

g) **aplicar**, mediante processo administrativo, eventuais **sanções administrativas** nos casos de ilícitos ou inadimplementos contratuais por parte da CONTRATADA (e seus prepostos, responsáveis e empregados), conforme fixado neste Termo de Referência e na legislação vigente;

h) **exigir**, durante toda a vigência do contrato, a **manutenção das condições de habilitação** em compatibilidade com as regras exigidas na licitação;

i) **alterar**, mediante aditamento, o **escopo do objeto** definido neste Termo, sempre no sentido de **melhor atender ao interesse público primário** e observados os limites legalmente fixados, mediante prévio pronunciamento da Fiscalização;

j) **assegurar** o acesso de pessoal autorizado pela CONTRATADA, desde que devidamente identificados, para a execução do objeto contratado, tomando todas as providências necessárias;

k) **controlar** as ligações realizadas, documentando as ocorrências havidas;

l) **registrar** eventuais ocorrências e anormalidades na prestação dos serviços;

m) **observar** as demais obrigações decorrentes da legislação correlata;

n) **cumprir** e fazer cumprir todas as demais disposições contidas neste Termo de Referência.

CLÁUSULA SÉTIMA - OBRIGAÇÕES E RESPONSABILIDADES DA CONTRATADA

A CONTRATADA obriga-se a:

a) **credenciar** por escrito, junto ao CONTRATANTE, um preposto idôneo com poderes de decisão para representar a empresa, principalmente no tocante à eficiência e agilidade da execução dos serviços objeto deste Termo de Referência;

b) **executar** os serviços contratados em estrita observância às especificações, condições, parâmetros e prazos definidos neste Termo de Referência, bem como observando as exigências e as solicitações e determinações da Fiscalização;

c) **fornecer** os softwares, equipamentos e acessórios necessários à execução dos serviços previstos neste Termo de Referência;

d) **responsabilizar-se** por todos os encargos comerciais, trabalhistas, fiscais e sociais decorrentes da contratação;

e) **responsabilizar-se** pela quitação e/ou cumprimento de eventuais sanções administrativas aplicadas pela CONTRATANTE em decorrência de ilícitos ou inadimplementos contratuais;

f) **cumprir** todos os prazos expressamente fixados neste Termo de Referência, bem com aqueles fixados diretamente pela Fiscalização;

g) **reparar ou corrigir**, às suas expensas, no total ou em parte, os serviços que compõem o escopo do objeto da Contratação em que se verificarem vícios, defeitos ou incorreções;

h) **responsabilizar-se** por quaisquer danos causados à CONTRATANTE ou a terceiros ocorridos durante a execução do objeto e em decorrência dela;

i) **apresentar** a documentação necessária à liquidação e pagamento da despesa para fins atestação da Fiscalização, observadas as regras fixadas neste Termo de Referência e na legislação vigente;

j) **manter-se**, durante a execução do Contrato, em compatibilidade com as condições de habilitação e qualificação exigidas na licitação;

k) **responder** por quaisquer interferências de estranhos nos acessos em serviço, bem como zelar pela integridade das comunicações;

l) **implantar**, de forma adequada, a supervisão permanente dos serviços, de modo a obter uma operação correta e eficaz;

m) **comunicar** ao CONTRATANTE, por escrito ou através de e-mail, qualquer anormalidade nos serviços e prestar os esclarecimentos julgados necessários;

n) **em nenhuma hipótese**, veicular publicidade ou qualquer outra informação acerca da prestação dos serviços do Contrato, sem prévia autorização do CONTRATANTE;

o) **responsabilizar-se** pelos ônus resultantes de quaisquer ações, demandas, custos e despesas decorrentes de danos, ocorridos por culpa sua ou de qualquer de seus empregados e prepostos obrigando-se, outrossim, por quaisquer responsabilidades decorrentes de ações judiciais movidas por terceiros, que lhe venham a ser exigidas por força da Lei, ligadas ao cumprimento do Contrato;

p) **observar** as demais obrigações decorrentes da legislação correlata;

q) **cumprir** outras exigências contidas neste Termo de Referência, bem como solicitações e determinações da Fiscalização;

r) **executar** outras atividades e procedimentos necessários ao fiel cumprimento das obrigações contratuais nos termos fixados neste Termo de Referência.

CLÁUSULA OITAVA - PRAZO DE VIGÊNCIA DO CONTRATO

O presente Contrato terá vigência de 12 (doze) meses, contados a partir da data de sua assinatura, e poderá ser prorrogado por iguais e sucessivos períodos com base no inciso II, art. 57 da Lei Federal 8.666/93.

Parágrafo Único - A quantidade estimada dos serviços consta na Planilha de Quantitativos e Valores Estimados - Anexo I do Termo de Referência do Edital do Pregão Presencial nº 17/2023 da ALPB e seus anexos.

CLÁUSULA NONA - DA RESCISÃO CONTRATUAL

A inexecução total ou parcial deste Contrato enseja a sua rescisão, conforme disposto nos artigos 77 a 80 da Lei nº 8.666/93 e alterações posteriores.

Parágrafo Primeiro - Os casos de rescisão contratual serão formalmente motivados nos autos do processo, assegurado o contraditório e a ampla defesa.

Parágrafo Segundo - A rescisão deste Contrato poderá ser:

a) Determinada, por ato unilateral e escrito da Administração da Contratante, nos casos enumerados nos incisos I a XII e XVII do artigo 78 da lei acima mencionada, notificando-se a Contratada com a antecedência mínima de 30 (trinta) dias, ou;
b) Amigável, por acordo entre as partes, reduzida a termo no processo licitatório, desde que haja conveniência para a Administração da Contratante, ou;
c) Judicial, nos termos da legislação vigente sobre a matéria.

Parágrafo Terceiro - A rescisão administrativa ou amigável será precedida de autorização escrita e fundamentada da Assembleia Legislativa da Paraíba.

CLÁUSULA DÉCIMA - DAS PENALIDADES

Pela inexecução total ou parcial da prestação de serviço objeto deste Contrato, a Contratante poderá, nos termos dos Artigos 86 e 87 da Lei 8.666/93 e alterações posteriores, garantida a prévia defesa, aplicar à Contratada as seguintes sanções, após o regular processo administrativo:

a) Advertência;
b) Multa de 0,5% (zero vírgula cinco por cento) do valor da fatura devida por dia de atraso no fornecimento/prestação do serviço contratado;
c) Multa de 5% (cinco por cento) do valor da contratação pelo descumprimento de qualquer obrigação contratual ou pela inexecução parcial do Contrato;
d) Multa de 10% (dez por cento) sobre o valor do Contrato, no caso de recusa injustificada da licitante vencedora em realizar a prestação do serviço no prazo estipulado em sua proposta e nas condições estabelecidas neste Contrato, ou ainda no caso de atraso superior a 30 (trinta) dias;
e) Suspensão temporária de participação em licitação e impedimento de contratar com a Administração, por prazo de até 05 (cinco) anos;

f) Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a sua reabilitação perante a Assembleia Legislativa, após o ressarcimento dos prejuízos que a licitante vier a causar, decorrido o prazo de sanção aplicada com base nesta Cláusula.

Parágrafo Primeiro - Na hipótese de a licitante, injustificadamente, não executar o serviço no prazo estipulado em sua proposta e nas condições estabelecidas no presente instrumento contratual, a Assembleia Legislativa poderá convocar as licitantes remanescentes na ordem de classificação para fazê-lo, em igual prazo e nas mesmas condições propostas pela primeira classificada, em conformidade com o art. 64, § 2º, da supramencionada Lei.

Parágrafo Segundo - As multas serão descontadas de pagamentos devidos pela Administração, ou quando for o caso, cobradas judicialmente.

Parágrafo Terceiro - Após a aplicação de qualquer penalidade prevista neste instrumento, realizar-se-á comunicação escrita à empresa e publicação no Órgão de Imprensa Oficial (excluídas as penalidades de advertência e multa de mora), constando o fundamento legal da punição.

Parágrafo Quarto - A sanção estabelecida na alínea d desta Cláusula será de competência exclusiva da Assembleia Legislativa, facultada sempre a defesa da Contratada no respectivo processo, nos termos do Parágrafo Terceiro do Art. 87 da lei nº 8.666/93 e alterações posteriores.

Parágrafo Quinto - Os valores das multas previstas nesta Cláusula deverão ser recolhidos diretamente à conta da Assembleia Legislativa e apresentado o comprovante à Procuradoria geral da Contratante.

CLÁUSULA DÉCIMA PRIMEIRA - DA PUBLICAÇÃO

Será de inteira responsabilidade da Contratante, providenciar, à sua conta, a publicação do extrato deste instrumento contratual na Impressa Oficial, até o 5º (quinto) dia útil do mês seguinte ao de sua assinatura, conforme o Parágrafo Único, do art. 61 da Lei nº 8.666/93 e alterações posteriores.

CLÁUSULA DÉCIMA SEGUNDA - DA ALTERAÇÃO DO CONTRATO

Este Contrato poderá ser alterado nos casos previstos no art. 65, da Lei nº 8.666/93 e alterações posteriores, desde que haja interesse da Contratante, com a apresentação das devidas justificativas, adequadas aos termos deste Contrato.

CLÁUSULA DÉCIMA TERCEIRA - DA SUBCONTRATAÇÃO

Os serviços **NÃO** poderão ser subcontratados com terceiros.

CLÁUSULA DÉCIMA QUARTA – DO REAJUSTE

O valor do contrato poderá ser reajustado a cada 12 (doze) meses, de acordo com o índice oficial do governo (ÍNDICE NACIONAL DE PREÇOS AO CONSUMIDOR AMPLO– IPCA) ou qualquer que vier a substituí-lo.

CLÁUSULA DÉCIMA QUINTA – DA FISCALIZAÇÃO DO CONTRATO

Parágrafo Primeiro - Para garantir maior racionalização e objetividade à execução do contrato de prestação do serviço, a **ASSEMBLEIA LEGISLATIVA DO ESTADO DA PARAÍBA** e a CONTRATADA deverão indicar, oficialmente, no ato da assinatura do contrato, profissionais que os representarão, passando a atuar como Fiscal e Preposto, respectivamente.

Parágrafo Segundo - Os aludidos representantes do contrato ficarão responsáveis pelas atividades de planejamento, coordenação e controle da execução de todo o projeto, além do acompanhamento do cumprimento dos prazos e metas estabelecidos, além da aprovação das faturas relativas à prestação dos serviços.

Parágrafo Terceiro - Ao Fiscal do Contrato nomeado pelo órgão CONTRATANTE caberá, entre outras atribuições:

a) Zelar para que as atividades a cargo do órgão CONTRATANTE sejam cumpridas dentro dos prazos estabelecidos;
b) Acompanhar execução dos serviços a cargo da CONTRATADA, permitindo, se necessário, sempre que informado previamente, o acesso dos técnicos às instalações das unidades da CONTRATANTE, de modo a possibilitar a execução das implantações, ampliações e manutenções preventivas, a fim de fazer cumprir o objeto licitado;
c) Zelar para que os serviços de manutenções corretivas sejam executados dentro dos prazos contratuais, com os respectivos registros dos códigos de abertura dos chamados, que garantirão o acesso dos técnicos às instalações das unidades do órgão CONTRATANTE;
d) Zelar para que os profissionais alocados pela CONTRATADA para prestação dos serviços só tenham acesso às dependências das unidades do órgão CONTRATANTE mediante apresentação de cartões de identificação profissional com fotografia e número de identidade;
e) Manter registro das atividades relacionadas ao desenvolvimento do contrato;
f) Agendar reuniões periódicas com a CONTRATADA para avaliação dos serviços prestados, recomendar alternativas de soluções para os problemas detectados, apontando eventuais deficiências verificadas na execução dos serviços e solicitando imediata correção, sem prejuízo da aplicação das penalidades previstas em contrato;
g) Conferir pormenorizadamente os valores cobrados nas faturas emitidas pela CONTRATADA.

Parágrafo Quarto - À CONTRATADA, através do Preposto do contrato, por ela nomeado, caberá, entre outras responsabilidades:

a) Assegurar o sigilo sobre as informações relativas ao órgão CONTRATANTE;
b) Zelar para que as atividades a cargo da CONTRATADA sejam cumpridas dentro dos prazos estabelecidos;
c) Assegurar a capacitação necessária das equipes responsáveis pela realização dos trabalhos;
d) Acompanhar a execução dos serviços, solicitando, quando necessário, o acesso de seus técnicos às instalações das unidades do órgão CONTRATANTE, de modo a possibilitar a execução das implantações, ampliações e manutenções preventivas, a fim de fazer cumprir o objeto licitado;
e) Zelar para que os serviços de manutenção/reparo corretivos sejam executados dentro dos prazos contratuais, mediante registros dos códigos de abertura dos chamados, que garantirão o acesso dos técnicos às instalações das unidades do órgão CONTRATANTE;
f) Zelar pela permanente manutenção dos equipamentos que compõem o objeto do contrato, garantindo boas condições de funcionamento, providenciando todos os ajustes, reparos e substituições de peças que se façam necessárias;
g) Garantir que nas substituições de equipamentos em operação, em caso de defeitos, os novos equipamentos operem com qualidade igual ou superior, pelo tempo necessário até a devolução do original, excetuando-se os casos previstos na cláusula anterior;
h) Zelar para que a remoção de quaisquer equipamentos em operação, quando necessária, seja comunicada previamente ao Fiscal do Contrato nomeado pelo órgão CONTRATANTE, bem como os motivos da retirada, a previsão de retorno e a devolução para os locais de origem;
i) Garantir que todos os profissionais alocados para prestação de serviço nas dependências do órgão CONTRATANTE apresentem cartões de identificação profissional com fotografia e número de identidade, para que tenham acesso controlado;
j) Providenciar imediata substituição, ante a expressa manifestação escrita do Fiscal do Contrato nomeado pelo

órgão CONTRATANTE, de quaisquer de seus profissionais encarregados da execução dos serviços, que não corresponderem aos princípios éticos e morais nas suas dependências;
k) Garantir que todas as atividades sejam realizadas dentro dos padrões de qualidade, segurança e higiene, observando os requisitos da medicina do trabalho e prevenção contra incêndios;
l) Manter registro das atividades relacionadas ao desenvolvimento do contrato;
m) Participar de reuniões periódicas com o CONTRATANTE para avaliação dos serviços prestados, apresentando soluções para os problemas detectados, adotando providências no sentido de superar eventuais deficiências verificadas na execução dos serviços.

CLÁUSULA DÉCIMA SEXTA - DAS DISPOSIÇÕES GERAIS

Os casos omissos e as dúvidas suscitadas durante a execução deste Contrato serão resolvidos pelas partes contratantes de comum acordo, observado o que dispõe a Lei nº 8.666/93 e alterações posteriores.

Parágrafo Primeiro - Ficará a cargo do **Departamento de Informática** desta Casa Legislativa o acompanhamento e controle da execução total deste Contrato.

a) A **gestão** do contrato ficará a cargo do **Departamento de Informática** desta Casa Legislativa, através do servidor **Brunno Ugulino de Araújo Maranhão, matrícula 280.255-4**, Diretor de Departamento, a quem competirá dirimir as dúvidas que surgirem no curso da execução do contrato e de tudo dará ciência à Administração.

b) A **fiscalização** do contrato ficará a cargo do **Departamento de Informática** desta Casa Legislativa, através do servidor **Rodrigo Martins de Moura, matrícula 280.931-1,** Diretor de redes e conectividades.

Parágrafo Segundo - Fica eleito o Foro da Cidade de João Pessoa, Estado da Paraíba, como competente para dirimir questões oriundas da execução deste Contrato.

E por estarem justas e Contratadas, as partes assinam, perante as testemunhas abaixo, o presente instrumento em 03 (três) vias de igual teor e forma para que produzam seus efeitos legais.

João Pessoa, ____ de _____ de 2023.

_____
ASSEMBLEIA LEGISLATIVA DAPARAÍBA
Bruno Mouzinho Regis
Diretor Geral

_____
Contratada

TESTEMUNHAS:

_____
_____