LICITAÇÃO N.º 21/2021

Pregão Eletrônico - Registro de Preços

Protocolo n.º 4578/2021 (PAD)

ABERTURA DA LICITAÇÃO

DIA 09/08/2021 às 16:00 HORAS

1 - O Tribunal Regional Eleitoral do Paraná, por meio do Pregoeiro designado pela Portaria nº 257/2019, da Secretaria do Tribunal Regional Eleitoral do Paraná - TRE/PR, torna público que fará realizar licitação, na **modalidade PREGÃO ELETRÔNICO, sob a forma de REGISTRO DE PREÇOS, tipo menor preço do lote,** regida pela Lei nº 10.520/02, Lei Complementar nº 123/06 e Lei nº 11.488/2007, pelos Decretos n.º 10.024/2019 e n.º 8.538/15, subsidiariamente pela Lei nº 8.666/93 e por outras normas aplicáveis ao objeto deste certame, de acordo com o presente edital e seus anexos.

1.1 - No dia **09 (nove) de agosto de 2021, às 16:00 horas**, horário de Brasília – DF, na Sala da Comissão Permanente de Licitação, do prédio do TRE-PR, sito na Rua João Parolin nº 224, Bairro Parolin, Curitiba-PR, será feita a abertura do certame, **exclusivamente por meio de sistema eletrônico** do Governo Federal que promove a comunicação pela Internet (*Comprasnet:* www.comprasgovernamentais.gov.br).

1.2 - Integram este edital, independente de transcrição, o **Termo de Referência - Anexo I, a Proposta Detalhada – Anexo II, o Termo de Sigilo e Responsabilidade – Anexo III, a Ata de Registro de Preços – Anexo IV e a Minuta do Contrato – Anexo V.**

2 - DO OBJETO

2.1 – A presente licitação tem como objeto a contratação de empresa especializada para **fornecimento de solução de comunicação**

(roteadores, licenças e serviço), visando atender às necessidades deste Tribunal Regional Eleitoral, de acordo com as especificações e condições descritas no Termo de Referência - Anexo I.

3 - DO CREDENCIAMENTO ESPECÍFICO DO PREGÃO ELETRÔNICO

3.1 – Poderão participar deste certame as empresas que atenderem às condições deste edital, inclusive quanto à documentação, e estiverem devidamente credenciadas no sistema *Comprasnet*, cujo gerenciamento (órgão provedor do sistema eletrônico) é feito pelo Ministério da Economia.

3.1.1 - A licitante deverá manter seus dados (email e telefone para contato) rigorosamente atualizados no Portal do sistema *Comprasnet*.

3.2 - Somente poderão participar desta licitação pessoas jurídicas legalmente estabelecidas no País, cujo objeto social expresso no estatuto ou contrato social especifique atividade pertinente e compatível com o objeto da presente licitação e que atendam às condições deste edital, desde que não estejam cumprindo as seguintes sanções previstas nos seguintes dispositivos legais:

a) Art. 7º da Lei nº 10.520/02;

b) Inciso III do art. 87 da Lei nº 8.666/93, quando aplicado por este Tribunal;

c) Inciso IV do art. 87 da Lei nº 8.666/93.

3.3 – Será permitida a participação de cooperativas, desde que apresentem modelo de gestão operacional adequado ao objeto desta licitação, com compartilhamento ou rodízio das atividades de coordenação e supervisão da execução dos serviços, e desde que os serviços contratados sejam executados obrigatoriamente pelos cooperados.

3.4 - As condições exigidas no item 3.2 e 3.3 serão verificadas pelo Pregoeiro em conjunto com a documentação de habilitação.

3.5 - Não poderão participar desta licitação empresas que tenham em seu quadro societário cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade até o terceiro grau, inclusive, dos magistrados ocupantes de cargos de direção ou no exercício de funções administrativas, assim como de servidores ocupantes de cargos de direção, chefia e assessoramento vinculados direta ou indiretamente às unidades situadas na linha hierárquica da área encarregada da licitação (art. 2º, inc. VI, da Resolução nº 07, de 18/10/2005, incluído pela Resolução nº 229, de 22/06/2016, ambas do Conselho Nacional de Justiça).

3.5.1 - A proibição constante do item acima se estende até 06 (seis) meses, contados da abertura da licitação, após a desincompatibilização do magistrado ou servidor gerador da incompatibilidade (art. 2º, § 3º, da Resolução nº 07, de 18/10/2005, incluído pela Resolução nº 229, de 22/06/2016, ambas do Conselho Nacional de Justiça).

3.6 - A contratação de empresa pertencente a parente de magistrado ou servidor não abrangido pelas hipóteses expressas de nepotismo poderá ser vedada por este Tribunal, quando, no caso concreto, seja identificado risco potencial de contaminação do processo licitatório. (art. 2º, § 4º, da Resolução nº 07, de 18/10/2005, incluído pela Resolução nº 229, de 22/06/2016, ambas do Conselho Nacional de Justiça).

3.7 - É vedada a manutenção, aditamento ou prorrogação de contrato de prestação de serviços com empresa que venha a contratar empregados que sejam cônjuges, companheiros ou parentes em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de ocupantes de cargos de direção e de assessoramento, de membros ou juízes vinculados a este Tribunal (art. 3º da Resolução nº 07, de 18/10/2005, com redação dada pela Resolução nº 09, de 06/12/2005, ambas do Conselho Nacional de Justiça).

3.8 - A licitante deverá manifestar o pleno conhecimento e atendimento às exigências de habilitação do presente edital, em campo próprio do sistema eletrônico, como requisito para participação no Pregão Eletrônico.

3.8.1 - Todos os custos decorrentes da elaboração e apresentação de propostas serão de responsabilidade exclusiva da licitante, incluindo as transações que forem efetuadas em seu nome no Sistema Eletrônico ou de eventual desconexão. O Tribunal Regional Eleitoral do Paraná não será responsável, em nenhum caso, pelos custos de tais procedimentos.

3.9 - A licitante deverá estar inscrita no sistema eletrônico *Comprasnet*, no site www.comprasgovernamentais.gov.br

3.9.1 - O credenciamento far-se-á pela atribuição de chave de identificação e de senha, pessoal e intransferível, para acesso ao sistema eletrônico.

3.9.2 - O credenciamento junto ao provedor do sistema implica a responsabilidade legal da licitante ou de seu representante legal e a presunção de sua capacidade técnica para realização das transações inerentes ao Pregão Eletrônico.

3.10 - O uso da senha de acesso ao sistema eletrônico é de inteira e exclusiva responsabilidade da licitante, incluindo qualquer transação efetuada diretamente ou por seu representante, não cabendo ao provedor do sistema ou ao TRE/PR responsabilidade por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros.

4 - ENVIO DAS PROPOSTAS DE PREÇOS[1] E DOCUMENTOS DE HABILITAÇÃO

4.1 - A participação no pregão eletrônico dar-se-á por meio da digitação da senha privativa da licitante e subsequente encaminhamento da proposta de preços, **no valor unitário de cada item**, bem como dos documentos de habilitação informados neste edital, caso haja, a partir da divulgação do edital até a data e hora da abertura da sessão pública, **exclusivamente por meio do sistema eletrônico**.

4.1.1 – Além dos documentos solicitados no item acima, as licitantes deverão encaminhar, via sistema, incluindo no sistema *Comprasnet*:

4.1.1.1 – Proposta detalhada, conforme modelo constante no Anexo II, onde constem discriminados todos os equipamentos que compõem a

[1] A licitante deverá **analisar detalhadamente** o edital (e anexos) para formular proposta/lance firme e possível de cumprimento, tendo em vista o Acórdão TCU nº 754-2015 – Plenário, que determinou instauração de processo com vistas à penalização das empresas que pratiquem, injustificadamente, ato ilegal tipificado no art. 7º da Lei nº 10.520/2002 na licitação.

solução, com os respectivos modelos e softwares necessários e política de garantia adicional oferecida pelo fabricante (caso haja).

4.1.2 – As licitantes poderão deixar de apresentar os documentos de habilitação que constem no SICAF.

4.1.3 - A licitante deverá encaminhar, também, as seguintes informações cadastrais por meio do sistema, em documento eletrônico próprio (anexo), sendo vedado o seu envio no campo da descrição detalhada do objeto, sob pena de desclassificação em razão da identificação da proposta antes dos lances:

a) Nome do representante legal que assinará o contrato:................
b) CPF do representante Legal: ....
c) Cargo que ocupa: ....
d) Telefone fixo: ....
e) Telefone celular:..................
f) E-mail: ....
g) Endereço completo (com CEP) para fins de faturamento: ....
h) Endereço completo (com CEP) para fins de envio de correspondência: ....

4.1.4 - Até a abertura da sessão pública, as licitantes poderão retirar ou substituir a proposta e os documentos de habilitação anteriormente apresentados.

4.2 - A licitante responsabilizar-se-á por todas as transações que forem efetuadas em seu nome no sistema eletrônico, assumindo como firmes e verdadeiras suas propostas, assim como os lances inseridos durante a sessão pública.

4.3 - Incumbirá à licitante acompanhar as operações no sistema eletrônico durante a sessão pública do pregão eletrônico, ficando responsável pelo ônus decorrente da perda de negócios diante da inobservância de qualquer mensagem emitida pelo sistema ou de sua desconexão.

4.4 - O valor unitário máximo aceitável para cada item que compõe o lote é de:

	ITEM	DESCRITIVO	QTDE	Valor máximo unitário aceitável
LOTE 01	1	ROTEADOR CONCENTRADOR	2	R$ 51.388,64
	2	ROTEADOR REMOTO SD-WAN COM WI-FI INTEGRADO	135	R$ 8.182,12
	3	PONTO DE ACESSO WI-FI	80	R$ 9.297,15
	4	SERVIÇO DE INSTALAÇÃO E SUPORTE	1	R$ 181.229,71

4.4.1 - As propostas deverão ser apresentadas pelo valor unitário do item, sendo que aquelas selecionadas ficarão à disposição da

Administração, que se valerá dos preços registrados para a aquisição dos produtos.

4.5 – A quantidade ofertada na proposta deverá corresponder ao quantitativo total estimado para cada item, conforme item 2.1 do Termo de Referência.

4.6 - Os preços propostos deverão ser finais, acrescidos de todas as despesas (fretes, impostos, taxas, etc.) e conter somente duas casas decimais, não sendo admitidos valores simbólicos, irrisórios ou iguais a zero, ensejando a desclassificação.

4.7 - O CNPJ cadastrado no sistema *Comprasnet*, para fins de participação no certame, deverá ser o mesmo para efeito de emissão das notas fiscais/faturas para posterior pagamento.

4.7.1 - Caso a licitante vencedora não possa emitir as notas fiscais/faturas com o mesmo CNPJ habilitado na licitação, poderá fazê-lo por meio de outra unidade (matriz ou filial) da mesma empresa. Nesse caso, ambos os CNPJs deverão estar com a documentação fiscal regular.

4.8 - Serão irrelevantes quaisquer ofertas que não se enquadrem nas especificações exigidas, ou anexos não solicitados, considerando-se que pelo preço proposto, a empresa obrigar-se-á ao fornecimento descrito neste edital.

4.9 - As propostas terão eficácia por 90 (noventa) dias, de acordo com o art. 6º da Lei nº 10.520/02, e a vigência da Ata de Registro de Preços é de 12 (doze) meses, contados da data registrada no SIASG

4.10 - Em razão do descritivo do Sistema *Comprasnet* (também reproduzido no documento “Relação de Itens”) não possuir o mesmo nível de detalhamento do objeto do certame, as propostas deverão atender às especificações constantes do Termo de Referência (Anexo I) deste Edital.

4.11 - Será solicitado, nesta fase, o envio eletrônico das declarações de inexistência de fato superveniente referente à habilitação, quanto a proibição de trabalho noturno, perigoso ou insalubre a menores de 18 (dezoito) anos e qualquer trabalho a menores de 16 (dezesseis) anos, salvo na condição de aprendiz, a partir de 14 (quatorze) anos, de cumprimento de reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social, com atendimento às regras de acessibilidade previstas na legislação, conforme disposto no art. 93 da Lei nº 8.213, de 24 de julho de 1991 e de atendimento aos requisitos legais estabelecidos no art. 3º da Lei Complementar 123/06 para microempresa, empresa de pequeno porte ou sociedade cooperativa[2], se for o caso (conforme item 9.3).

4.12 - As declarações citadas nos itens acima somente serão visualizadas pelo Pregoeiro na fase de habilitação.

5 - DA ABERTURA DAS PROPOSTAS/SESSÃO PÚBLICA

5.1 – O Pregoeiro iniciará a sessão pública na data e horário previstos neste edital, via sistema eletrônico, com a divulgação das propostas de preços recebidas, no prazo avençado, as quais deverão estar em perfeita consonância com as especificações detalhadas no presente edital.

[2] art. 34 da Lei nº 11.488/2007.

6 - DA CLASSIFICAÇÃO INICIAL DAS PROPOSTAS

6.1 - Após a abertura da Sessão, o Pregoeiro verificará as propostas apresentadas e desclassificará, motivadamente e registrando no sistema, aquelas que não estiverem em conformidade com os requisitos estabelecidos neste Edital, com acompanhamento em tempo real por todos os participantes.

6.2 - Somente as licitantes com propostas classificadas participarão da fase de lances.

7 - DA FORMULAÇÃO DE LANCES

7.1 - A partir do início da Sessão Pública, as licitantes poderão encaminhar lances exclusivamente por meio do sistema eletrônico, sendo a licitante imediatamente informada do seu recebimento e respectivo horário de registro e valor.

7.1.1 - Os lances serão ofertados pelo **valor UNITÁRIO do item.**

7.2 - A licitante poderá oferecer lances sucessivos, observando o horário fixado e as regras de aceitação dos mesmos.

7.2.1 - A licitante só poderá ofertar lance inferior ao último por ela ofertado e registrado no sistema, observado o intervalo mínimo de diferença de valores de **R$ 100,00 (cem reais)** entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta.

7.3 - Em havendo dois ou mais lances de igual valor, prevalecerá o lance que for registrado em primeiro lugar.

7.4 – Embora a classificação final seja pelo valor total do lote, a disputa será por item e os lances ofertados devem estar dentro do valor estimado constante nesse edital. A cada lance ofertado por item, o sistema atualizará automaticamente o valor total do lote, sagrando-se vencedora a licitante que ofertar o menor valor total do lote.

7.5 - No transcurso da sessão pública, a licitante será informada, em tempo real do valor do menor lance registrado.

7.6 - Nesta fase o Pregoeiro poderá excluir, justificadamente, lance de valor considerado inexequível.

7.7 – Para o envio de lances será adotado o **modo de disputa aberto**, descrito a seguir:

7.7.1 - A etapa de envio de lances durará 10 (dez) minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos 2 (dois) minutos do período de duração da Sessão Pública.

7.7.2 - A prorrogação automática da etapa de envio de lances de que trata o item anterior, será de 2 (dois) minutos e ocorrerá, sucessivamente, sempre que houver lances enviados nesse período de prorrogação, inclusive quando se tratar de lances intermediários.

7.7.3 - Na hipótese de não haver novos lances na forma estabelecida no item 7.7.1, a Sessão Pública será encerrada automaticamente

7.7.4 - Encerrada a Sessão Pública sem prorrogação automática pelo sistema, nos termos do disposto no item 7.7.2, o Pregoeiro poderá, assessorado pela equipe de apoio, admitir o reinício da etapa de envio de lances, em prol da consecução do melhor preço, mediante justificativa.

7.8 - No caso de desconexão com o Pregoeiro, no decorrer da etapa competitiva do Pregão Eletrônico, o sistema eletrônico poderá permanecer acessível às licitantes para a recepção dos lances, retornando o Pregoeiro, quando possível, sua atuação no certame, sem prejuízo dos atos realizados.

7.8.1 - Quando a desconexão persistir por tempo superior a 10 (dez) minutos, a sessão do Pregão Eletrônico será suspensa e terá reinício somente decorridas 24 (vinte e quatro) horas após a comunicação do fato aos participantes, no sítio eletrônico usado para divulgação.

7.9 - Não se admitirá proposta que apresente preços simbólicos, irrisórios ou de valor zero, ensejando a desclassificação.

7.10 - Os preços apresentados deverão ser compatíveis com a conjuntura do mercado, sendo que a apresentação da proposta implica a aceitação de todas as condições deste edital.

8 - DA ACEITAÇÃO DAS PROPOSTAS

8.1 - Encerrada a etapa de envio de lances da Sessão Pública, o Pregoeiro encaminhará, pelo sistema eletrônico, contraproposta ao licitante que tenha apresentado o melhor preço, para que seja obtida melhor proposta, vedada a negociação em condições diferentes das previstas neste edital.

8.2 - Caso haja propostas apresentadas por microempresas, empresas de pequeno porte ou cooperativas, iguais ou até 5% superiores à proposta detentora do melhor lance e não sendo esta ME, EPP ou cooperativas, será assegurada preferência de contratação, respeitado o que segue:

a) A microempresa, empresa de pequeno porte ou cooperativas melhor classificada, poderá apresentar proposta de preço inferior àquela detentora do melhor lance, no prazo máximo de 5 (cinco) minutos, após o encerramento dos lances, controlados pelo sistema, sob pena de preclusão.

b) Caso o lance ofertado, conforme condições do item anterior, seja inferior ao menor lance original, o objeto será adjudicado em favor da microempresa ou empresa de pequeno porte, se habilitada.

c) Não ocorrendo à contratação da microempresa, empresa de pequeno porte ou cooperativas na forma do subitem anterior, serão convocadas as demais ME ou EPP que se enquadrem na condição prevista, na ordem classificatória, para a manifestação do mesmo direito.

d) Caso o empate persista até o encerramento do item, o Sistema fará um sorteio eletrônico entre os fornecedores envolvidos, definindo e convocando, automaticamente, a vencedora para o encaminhamento da oferta final de desempate.

8.2.1 - Na hipótese de nenhuma empresa classificada exercer o direito de preferência, o objeto será adjudicado em favor da proposta originalmente vencedora do certame, conforme item 8.3 e seguintes.

8.3 – O não encaminhamento dos documentos solicitados no item 4.1.1, deste edital, ou sua não aprovação ensejará à desclassificação, sendo convocada a licitante classificada em 2º lugar para atender ao disposto acima e assim sucessivamente.

8.3.1 – A licitante deverá encaminhar os documentos constantes no item 4.1.1 devidamente configurados, e em formato para impressão.

8.4 – Após o encerramento da etapa de lances, o Pregoeiro efetuará a aceitação da proposta de **MENOR PREÇO DO LOTE**.

8.4.1 – Não será aceita proposta cujo quantitativo ofertado seja inferior ao estabelecido no item 2.1 do Termo de Referência – Anexo I.

8.4.2 – Para a aceitação da proposta, a licitante deverá atentar para o fato de que todos os valores deverão conter, OBRIGATORIAMENTE, apenas 02 (duas) casas decimais.

8.4.3 – Caso a proposta da licitante não contenha apenas duas casas decimais, o Pregoeiro efetuará a divisão para que se obtenha a referida adequação.

8.5 – Na hipótese da proposta ou do lance de menor valor não ser aceito ou se a licitante vencedora desatender às exigências habilitatórias, o Pregoeiro examinará a proposta ou lance subsequente, verificando a sua aceitabilidade e procedendo a sua habilitação na ordem de classificação, segundo o critério do **menor preço unitário do item** e assim, sucessivamente até a apuração de uma proposta ou lance que atenda ao edital.

8.5.1 – Ocorrendo a hipótese anterior, o Pregoeiro negociará com a licitante, no sentido de se obter preço melhor.

8.6 – Serão desclassificadas as propostas de preços que:

a) não atenderem às exigências deste edital;

b) apresentarem, após a fase de lances ou negociação, valores superiores aos estabelecidos para a presente contratação ou preços manifestamente inexequíveis.

8.6.1 – Considerar-se-ão preços manifestamente inexequíveis, de que trata o item anterior, aqueles que, comprovadamente, levem a valores insuficientes para a cobertura dos custos decorrentes da contratação pretendida.

8.6.2 – Havendo indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderá ser efetuada diligência, na forma do § 3º do art. 43 da Lei nº 8.666/93, para efeito de comprovação de sua exequibilidade.

9 – DA HABILITAÇÃO

9.1 – Em conjunto com o exame da documentação de habilitação do licitante detentor da proposta classificada em primeiro lugar, o Pregoeiro verificará o eventual descumprimento das condições de participação, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, conforme disposto no item 3.2, mediante a consulta aos seguintes cadastros:

9.1.1 - SICAF;

9.1.2 – Consulta Consolidada de Pessoa Jurídica - Tribunal de Contas da União (https://certidoes-apf.apps.tcu.gov.br/).

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

9.2 - Para habilitação na presente licitação, a licitante deverá estar cadastrada no SICAF, com a documentação regularizada, comprovando regularidade para com a Fazenda Federal, Seguridade Social e ao Fundo de Garantia por Tempo de Serviço, nos termos do art. 29 da Lei nº 8.666/93, sendo a comprovação desta habilitação obtida *on line* pelo Pregoeiro, que verificará a validade dos documentos.

9.2.1 - Caso conste no cadastro do SICAF algum documento habilitatório com data de validade expirada, o Pregoeiro poderá consultar o documento da licitante vencedora nas páginas (sítios) das entidades responsáveis pelo referido tributo.

9.2.1.1 – Caso o Pregoeiro não logre êxito em obter a certidão correspondente por meio do sítio oficial, ou na hipótese de ela se encontrar vencida no referido sistema, o licitante será convocado a anexar, em campo próprio do Sistema *Comprasnet*, no prazo de 02 (duas) horas a contar da solicitação, documento válido que comprove o atendimento das exigências deste Edital, sob pena de inabilitação[3].

9.2.2 – Para as microempresas e empresas de pequeno porte ou cooperativa, havendo alguma restrição na comprovação da regularidade fiscal, será assegurado o prazo de 5 (cinco) dias úteis, prorrogáveis por igual período a critério da Administração Pública, cujo termo inicial corresponderá ao momento em que o proponente for declarado o vencedor do certame, para a regularização da documentação, pagamento ou parcelamento do débito, e emissão de eventuais certidões negativas ou positivas com efeito de certidão negativa.

9.2.2.1 - A não-regularização da documentação, no prazo previsto acima, implicará decadência do direito à contratação, sem prejuízo das sanções previstas, sendo facultado à Administração convocar as licitantes remanescentes, na ordem de classificação.

9.2.3 - No caso de sociedades cooperativas deverão ser apresentados, ainda:

a) ata de fundação;
b) estatuto social com a ata da assembleia que o aprovou;
c) regimento dos fundos instituídos pelos cooperados, com a ata da assembleia que os aprovou;
d) editais de convocação das três últimas assembleias gerais extraordinárias;
e) três registros de presença dos cooperados que executarão o contrato em assembleias gerais ou nas reuniões seccionais;
f) ata da sessão em que os cooperados autorizam a cooperativa a contratar o

[3] Conforme IN 03/2018 SICAF.

objeto da licitação;

g) relação dos cooperados que atendem aos requisitos técnicos para a contratação e execução do contrato, com as respectivas atas de inscrição e a comprovação de que estão domiciliados na localidade da sede da cooperativa, respeitado o disposto no inciso XI do art.4º, inciso I do art. 21 e §§ 2º a 6º do art. 42 da Lei nº 5.764 de 1971;
h) a declaração de regularidade de situação do contribuinte individual (DRSCI) de cada um dos cooperados relacionados;
i) a comprovação do capital social proporcional ao número de cooperados necessários à prestação do serviço;
j) o registro previsto no art. 107 da Lei nº 5.764, de 1971;
k) a comprovação de integração das respectivas quotas-partes por parte dos cooperados que executarão o contrato;
l) a comprovação do envio do Balanço Geral e o Relatório do Exercício Social ao órgão de controle, conforme dispõe o art. 112 da Lei nº 5.764 de 1.971.

9.3 - Além do cadastro no SICAF, exigir-se-á das licitantes as declarações de inexistência de fato superveniente referente à habilitação, do cumprimento ao disposto no artigo 7º, inc. XXXIII da Constituição Federal, quanto a proibição de trabalho noturno, perigoso ou insalubre a menores de 18 (dezoito) anos e qualquer trabalho a menores de 16 (dezesseis) anos, salvo na condição de aprendiz, a partir de 14 (quatorze) anos e declaração de atendimento aos requisitos legais para a qualificação como microempresa, empresa de pequeno porte ou sociedade cooperativa[4], se for o caso, declaração de cumprimento de reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social, com atendimento às regras de acessibilidade previstas na legislação, conforme disposto no art. 93 da Lei nº 8.213, de 24 de julho de 1991 (tal exigência será feita no momento da elaboração e envio da proposta, por meio eletrônico, conforme item 4.11).

9.4 - Os documentos complementares à habilitação, quando necessários à confirmação daqueles exigidos no edital e já apresentados, deverão ser encaminhados em formato digital, via sistema, no prazo de 2 (duas) horas, após solicitação do Pregoeiro no sistema eletrônico.

9.5 - Se a documentação de habilitação não estiver completa e correta ou contrariar qualquer dispositivo deste edital e seus anexos, o Pregoeiro considerará a licitante inabilitada, a qual poderá sofrer as sanções cabíveis.

9.6 - Após a homologação correspondente, os preços serão registrados para futura utilização pelo Tribunal Regional Eleitoral do Paraná.

9.7 - Os demais procedimentos da fase externa do Pregão correrão conforme o disposto na Lei nº 10.520/02, artigo 4º e seus incisos.

10 – DOS DOCUMENTOS A SEREM ENTREGUES APÓS A ASSINATURA DO CONTRATO[5]

10.1 – No prazo de até, 5 (cinco) dias úteis após a assinatura do contrato, a contratada deverá entregar para o gestor do contrato:

a) o Termo de Sigilo e Responsabilidade (conforme modelo constante no **anexo III**), garantindo o cumprimento da Política de Segurança da Informação da Justiça Eleitoral.

[4] Art. 34 da Lei nº 11.488/2007
[5] Sem prejuízo de demais documentos que eventualmente sejam solicitados neste edital e seus anexos

a.1) O documento acima referido deverá ser preenchido e assinado pelo Representante Legal da empresa.

b) Comprovação de que os técnicos que irão realizar os serviços tenham a qualificação profissional necessária e sejam certificados pelo fabricante do equipamento, conforme item 2.3.4, subitem 6 do Termo de Referência – Anexo I.

11 - DA POSSIBILIDADE DE REDUÇÃO DE PREÇOS E FORMAÇÃO DO CADASTRO DE RESERVA

11.1 – O Cadastro de Reserva será formado por meio do registro das licitantes que aceitarem cotar os bens ou serviços com preços iguais aos da licitante vencedora, para futura contratação, no caso da impossibilidade de atendimento pelo primeiro colocado da Ata, atendendo ao disposto no art. 11 do Decreto nº 7.892/2013.

11.1.1 – A convocação para formação do Cadastro de Reserva será feita por meio de *email*, gerado pelo próprio Sistema C*omprasnet*.

11.1.2 – Ao final do processo, o referido Cadastro de Reserva poderá ser visualizado na consulta pública de visualização da Ata, juntamente com as demais informações como "Resultado por Fornecedor", "Declarações", "Termo de Homologação", etc.

11.2 - A apresentação de novas propostas na forma do item 11.1 não prejudicará o resultado do certame em relação à licitante melhor classificada.

11.3 - Quando houver a necessidade de contratação, serão observados os procedimentos de aceitabilidade das propostas bem como avaliadas as condições de habilitação das licitantes, conforme itens 8 e 9 deste edital.

12 – DOS ESCLARECIMENTOS E DA IMPUGNAÇÃO DO ATO CONVOCATÓRIO

12.1. – O prazo para envio de pedidos de esclarecimentos é de até 03 (três) dias úteis anteriores à data da abertura da Sessão.

12.2 – O Pregoeiro responderá aos pedidos de esclarecimentos no prazo de 02 (dois) dias úteis, contados da data de recebimento do pedido.

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

12.4 - Até 03 (três) úteis antes da data fixada para a abertura da Sessão Pública, qualquer pessoa poderá impugnar os termos do edital, por meio eletrônico, pelo e-mail cpl@tre-pr.jus.br, sendo necessário que o arquivo seja encaminhado na extensão ".doc", possibilitando a inserção no sistema *Comprasnet* pelo pregoeiro.

13 - DA FORMALIZAÇÃO DA ATA DE REGISTRO DE PREÇOS

13.1 - Após a homologação, o gestor da contratação convocará a licitante vencedora para assinar a Ata de Registro de Preços, no prazo máximo de 5 (cinco) dias úteis, contados da convocação.

13.1.1 - O prazo para a assinatura estabelecido no item anterior poderá ser prorrogado, desde que ocorra motivo justificado e aceito por este Tribunal.

13.2 - No caso da licitante vencedora, bem como as licitantes que reduziram seus preços, nos termos do item 11, após convocadas, não comparecerem ou se recusarem a assinar a Ata de Registro de Preços, sem prejuízo das punições previstas neste Edital e seus Anexos, a Administração poderá convocar as licitantes remanescentes, na ordem de classificação, para fazê-lo em igual prazo e nas mesmas condições.

13.3 - A Ata de Registro de Preços terá efeito de compromisso de fornecimento nas condições estabelecidas neste edital e seus anexos.

13.4 - A existência de preços registrados não obriga a Administração a firmar as contratações que deles poderão advir, não cabendo direito à indenização de qualquer espécie. Fica facultada a utilização de outros meios, respeitada a legislação pertinente às licitações e ao Sistema de Registro de Preços, assegurando-se, ao beneficiário do registro, preferência em igualdade de condições.

13.5 - Observados os critérios e condições estabelecidas no presente edital, a Administração poderá comprar de mais de um fornecedor registrado, segundo a ordem de classificação, desde que razões de interesse público justifiquem e que o primeiro classificado não possua capacidade de fornecimento compatível com o solicitado pela Administração, observadas as condições do edital e o preço registrado.

13.6 – Não será permitida a adesão à Ata de Registro de Preços por órgãos ou entidades não participantes.

14 - DA ATA COMPLEMENTAR

14.1 - Na hipótese da empresa vencedora ou aquelas que aceitaram reduzir seus preços, após cumprido do contido no item 11.1, não assinarem a Ata de Registro de Preços será possível, mediante a geração de Ata Complementar, a aplicação do procedimento previsto no parágrafo único do art. 13 do Decreto nº 7.892/2013.

14.2 - As empresa citadas acima, inadimplentes, não estarão isentas das penalidades previstas no edital.

15 – DA DESPESA ORÇAMENTÁRIA

15.1 - A despesa com a presente licitação correrá à conta dos elementos que serão especificados quando da solicitação dos itens.

15.2 - Uma vez homologado/adjudicado o item à empresa vencedora, solicitado pelo gestor da Ata e devidamente autorizado pela Diretoria Geral, a Secretaria de Orçamento e Finanças, procederá a emissão da NOTA DE EMPENHO, notificando-a para que manifeste o aceite respectivo.

15.2.1 - A empresa deverá manifestar o aceite da Nota de Empenho, no prazo máximo de 24 (vinte e quatro) horas, contados do comunicado feito pelo TRE.

15.2.2 - Não ocorrendo aceite da Nota de Empenho no prazo determinado no item acima, injustificadamente, a empresa estará sujeita às penalidades cabíveis.

16 – DO PAGAMENTO

16.1 – O pagamento do objeto da presente licitação será efetuado conforme disposições constantes do contrato (minuta anexa).

17 – DAS SANÇÕES ADMINISTRATIVAS

17.1 – Durante a fase externa da licitação[6], os licitantes estarão sujeitos à(s) penalidade(s) prevista(s) no art. 7º da Lei nº 10.520/2002, que dispõe que: "*quem, convocado dentro do prazo de validade da sua proposta, não celebrar o contrato, deixar de entregar ou apresentar documentação falsa exigida para o certame, ensejar o retardamento da execução de seu objeto, não mantiver a proposta, falhar ou fraudar na execução do contrato, comportar-se de modo inidôneo ou cometer fraude fiscal, ficará impedido de licitar e contratar com a União, Estados, Distrito Federal ou Municípios e, será descredenciado no SICAF, ou nos sistemas de cadastramento de fornecedores a que se refere o inciso XIV do art. 4º desta Lei, pelo prazo de até 5 (cinco) anos, sem prejuízo das multas previstas em edital e no contrato e das demais cominações legais*."

17.2 - As licitantes que praticarem as seguintes condutas, injustificadamente, estarão sujeitas à sanção de impedimento de licitar e contratar com a União, citada no item anterior, pelo prazo a seguir fixado:

a) Solicitar a desclassificação de sua proposta, após a etapa de lances: 01 (um) mês;

b) Deixar de entregar documentos exigidos na fase de aceitação da proposta: 02 (dois) meses;

c) Deixar de entregar documentos durante a fase de habilitação: 03 (três) meses;

17.2.1 - Poderá ser aplicada a penalidade de advertência às faltas leves, de menor gravidade, que não acarretarem prejuízo de monta ao interesse do serviço.

17.2.2 - Reputar-se-ão comportamentos inidôneos, para os fins do disposto no art. 7º da Lei nº 10.520/2002, atos como os descritos nos artigos 90, 92, 93, 94, 95, 96 e 97 da Lei nº 8.666/93.

17.3 - Nos termos da Lei nº 8.666/93 e da Lei nº 10.520/02, fica a licitante vencedora sujeita às penalidades previstas na minuta do contrato (anexo V deste edital).

17.4 - Pela recusa em assinar a Ata de Registro de Preços ou o instrumento contratual, a licitante vencedora estará sujeita à aplicação de multa de 20% (vinte por cento) sobre o valor total homologado.

17.5 - As multas imputadas à Contratada cujo montante seja superior ao mínimo estabelecido pelo Ministério da Economia [e] não pagas no prazo concedido pela Administração, serão inscritas em Dívida Ativa da União e cobradas com base na Lei 6.830/80, sem prejuízo da correção monetária pelo IGP-M ou outro

---

[6] Conforme entendimento firmado pelo TCU, no Acórdão nº 754/2015 – Plenário.

índice que por ventura venha a substituí-lo.

18 – DOS RECURSOS

18.1 – Das decisões proferidas pelo Pregoeiro, caberão recursos nos termos do artigo 44 e parágrafos do Decreto nº 10.024/2019.

18.2 – A empresa licitante poderá apresentar razões do recurso no prazo de 3 (três) dias, no momento da divulgação do vencedor, desde que manifestado imediata e motivadamente a intenção de recorrer, ficando as demais licitantes desde logo intimadas para apresentar contrarrazões em igual número de dias, que começarão a correr do término do prazo do recorrente, sendo-lhes assegurada vista dos autos, na Sala de Licitações do prédio do TRE/PR.

18.2.1 – Os procedimentos citados no item anterior serão realizados exclusivamente no âmbito do sistema eletrônico.

18.3 – A falta de manifestação imediata e motivada importará na decadência do direito de recurso e adjudicação do objeto pela Pregoeiro ao vencedor.

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

18.5 – Os recursos administrativos correspondentes à fase contratual correrão de acordo com os procedimentos especificados no artigo 109 da lei nº 8.666/93.

19 – DISPOSIÇÕES GERAIS

19.1 – O pregoeiro poderá, no julgamento da habilitação e das propostas, o sanar erros ou falhas que não alterem a substância das propostas, dos documentos e sua validade jurídica, nos termos do art. 47 do Decreto 10.024/2019.

19.2 – Para efeito de envio de documentos a serem inseridos no sistema Comprasnet, considera-se o horário das 12h às 18h.

19.3 - No caso de processo administrativo e durante o seu transcurso, as notificações às empresas poderão ser efetivadas por meio eletrônico, tais como e-mail ou aplicativo *Whatsapp*, presumindo-se eficaz a sua realização com o aviso de confirmação de recebimento do documento.

19.4 – Este Tribunal reserva-se o direito de optar pela adjudicação à empresa colocada em segundo lugar, e assim sucessivamente, se a primeira colocada não apresentar os documentos exigidos ou não atender as qualificações do presente edital, sujeitando-se a empresa recusante às penalidades legais cabíveis.

19.5 – O Tribunal Regional Eleitoral do Paraná poderá anular ou revogar a presente licitação, no todo ou em parte, conforme previsto em lei.

20 – INFORMAÇÕES

20.1 – Será possível a realização do *download* de todos os arquivos pertinentes a este edital por meio da internet, *home page*: www.tre-pr.jus.br.

20.2 – Outras informações e esclarecimentos relativos à licitação e condições poderão ser obtidos na Rua João Parolin nº 224, Sala da Comissão Permanente de Licitação, ou ainda:

- Pregoeiro/Equipe de Apoio: pelo telefone (41) 3330-8741 / 3330-8450 ou *e-mail* cpl@tre-pr.jus.br.

- Seção de Licitações: pelos telefones (41) 3330-8598 / 3330-8753 / 3072-4796, ou e-mail slic@tre-pr.jus.br.

20.2.1 – O horário para atendimento é de segunda a sexta-feira das 12h às 19h.

Curitiba, 27 de julho de 2021.

Julian Velloso Pugh
Pregoeiro

Anexo I

TERMO DE REFERÊNCIA

1 - OBJETO

1.1 – Registro de Preços para Aquisição de Solução de comunicação (roteadores, licenças e serviço), visando atender às necessidades deste Tribunal Regional Eleitoral, conforme especificações descritas no presente Termo de Referência.

2 – DAS ESPECIFICAÇÕES TÉCNICAS

2.1 – Poderão ser adquiridos os itens conforme quantitativo e especificações mínimas a seguir descritas:

Lote	ITEM	Descrição	Quantidade
1	1	ROTEADOR CONCENTRADOR – Código SIASG 104620	2
	2	ROTEADOR REMOTO SD-WAN COM WI-FI INTEGRADO - Código SIASG 104620	135
	3	PONTO DE ACESSO WI-FI - Código SIASG 393277	80
	4	SERVIÇO DE INSTALAÇÃO E SUPORTE - Código SIASG 26972	1

2.2 – A presente contratação se destina a aquisição de equipamentos para continuidade do processo de implantação da solução de comunicação para interligação dos Cartórios Eleitorais e do Edifício Sede do Tribunal Regional Eleitoral do Paraná, visando o bom funcionamento da rede. Considerando a necessidade de integração entre os equipamentos na solução pretendida, todos devem pertencer a um lote único, de forma a garantir a integração e o bom funcionamento da solução pretendida.

2.2.1 - Considerando que a presente licitação destina-se a dar continuidade à modernização da rede de dados da Justiça Eleitoral do Paraná iniciada em 2020, solicita-se que os equipamentos a serem licitados sejam do **fabricante Fortinet**. Desta forma será possível garantir a interoperabilidade entre os componentes e proteger o investimento já efetuado pelo TRE-PR.

2.2.2 – Segue, na tabela abaixo, a marca e modelo dos equipamentos a serem adquiridos nos itens 1, 2 e 3:

ITEM	Descrição	Marca e Modelo
1	ROTEADOR CONCENTRADOR	FortiGate 100F
2	ROTEADOR REMOTO SD-WAN COM WI-FI INTEGRADO	FortiWiFi 40F
3	PONTO DE ACESSO WI-FI	FortiAP 231F

2.3 – Das especificações dos itens a serem contratados:

2.3.1 - Item 1 – Roteador Concentrador

2.3.1.1 - Características do Equipamento:

1. Deve suportar, no mínimo, 10 Gbps com a funcionalidade de firewall habilitada para tráfego IPv4 e IPv6;
2. Deve suportar, no mínimo, 2 Gbps de throughput IPS;
3. Deve suportar, no mínimo, 8,5 Gbps de throughput de VPN IPSec;
4. Deve suportar, no mínimo, 1 Gbps de throughput de Inspeção SSL ou TLS;
5. Deve suportar, no mínimo, 1 Gbps de throughput com as funcionalidades firewall, controle de aplicação, IPS e antimalware habilitadas simultaneamente, para todas as assinaturas que a plataforma de segurança possuir;
6. Suporte a, no mínimo, 1.200.000 de conexões simultâneas;
7. Suporte a, no mínimo, 50.000 novas conexões por segundo;
8. Estar licenciado para, ou suportar sem o uso de licença adicional, 2.000 túneis de VPN IPSEC Site-to-Site simultâneos;
9. Estar licenciado para, ou suportar sem o uso de licença adicional, 15.000 túneis de clientes VPN IPSEC simultâneos;
10. Estar licenciado para, ou suportar sem o uso de licença adicional, 500 clientes de VPN SSL simultâneos;
11. Possuir ao menos 8 interfaces 1Gbps RJ-45;
12. Possuir ao menos 2 interfaces 10Gbps;
13. Estar licenciado ou ter disponível sem custo adicional, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance;
14. Suporte a, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance;
15. Possuir fonte de alimentação 100-240V AC;

16. Possuir no máximo 2 RU de altura.
17. Considerando que a presente contratação tem o objetivo de dar continuidade ao projeto de modernização da rede iniciado em 2020, para atendimento aos requisitos de compatibilidade e padronização da solução, os equipamentos a serem fornecidos neste item devem ser do fabricante Fortinet, modelo FortiGate 100F, ou superior.

2.3.1.2 – Requisitos mínimos de funcionalidade:

2.3.1.2.1 - Características Gerais:

1. A solução deve consistir em plataforma de proteção de rede baseada em appliance com funcionalidades de Next Generation Firewall (NGFW), e console de gerência e monitoração;
2. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;
3. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação;
4. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
5. Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19”, incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;
6. A gestão do equipamento deve ser compatível através da interface de gestão Web no mesmo dispositivo de proteção da rede, ou por console de gerenciamento instalada em máquina virtual compatível com solução VMWare em uso pelo TRE-PR;
7. Os dispositivos de proteção de rede devem possuir suporte a, pelo menos, 4000 VLAN Tags 802.1q;
8. Os dispositivos de proteção de rede devem possuir suporte a agregação de links 802.3ad e LACP;
9. Os dispositivos de proteção de rede devem possuir suporte a Policy based routing ou policy based forwarding;
10. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);

11. Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay;
12. Os dispositivos de proteção de rede devem possuir suporte a DHCP Server;
13. Os dispositivos de proteção de rede devem suportar sFlow;
14. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;
15. Deve suportar NAT dinâmico (Many-to-1);
16. Deve suportar NAT dinâmico (Many-to-Many);
17. Deve suportar NAT estático (1-to-1);
18. Deve suportar NAT estático (Many-to-Many);
19. Deve suportar NAT estático bidirecional 1-to-1;
20. Deve suportar Tradução de porta (PAT);
21. Deve suportar NAT de Origem;
22. Deve suportar NAT de Destino;
23. Deve suportar NAT de Origem e NAT de Destino simultaneamente;
24. Deve poder combinar NAT de origem e NAT de destino na mesma política;
25. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
26. Deve implementar o protocolo ECMP;
27. Deve permitir monitorar via SNMP falhas de hardware, uso de recursos, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster e estatísticas de uso das interfaces de rede;
28. Deve ser capaz de enviar logs para sistema de monitoramento externo e ser compatível com o software QRadar, utilizado pelo TRE-PR;
29. Deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2) para o protocolo IPv4;
30. Deve suportar roteamento dinâmico para o protocolo IPv6;
31. Suportar OSPF graceful restart;
32. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
33. Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;

34. Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;
35. Suporte a configuração de alta disponibilidade Ativo/Passivo ou Ativo/Ativo em modo transparente;
36. Suporte a configuração de alta disponibilidade Ativo/Passivo ou Ativo/Ativo em layer 3;
37. A configuração em alta disponibilidade deve sincronizar:
    a. Sessões;
    b. Configurações;
    c. NAT;
    d. QoS;
    e. Objetos de rede;
    f. Associações de Segurança das VPNs;
    g. Tabelas FIB;
38. O modo de alta disponibilidade deve possibilitar monitoração de falha de link;
39. Deve possuir suporte para criação de sistemas virtuais no mesmo appliance;
40. Deve permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados por equipes distintas;
41. Deve permitir o controle, inspeção e descriptografia de SSL para tráfego de entrada (Inbound) e Saída (Outbound), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos);
42. A solução deve identificar potenciais vulnerabilidades e destacar as melhores práticas que poderiam ser usadas para melhorar a segurança e o desempenho geral de uma rede;

2.3.1.2.2 - Controle por Política de Firewall

1. Deverá suportar controles por zona de segurança;
2. Deve permitir efetuar controles de políticas por porta e protocolo;

3. Deve permitir efetuar controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;
4. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
5. Firewall deve ser capaz de aplicar a inspeção UTM (Application Control e Webfiltering no mínimo) diretamente às políticas de segurança versus via perfis;
6. Deve suportar o padrão de indústria 'syslog' protocol para armazenamento usando o formato Common Event Format (CEF);
7. Deve suportar objetos de endereço IPv4 e IPv6, consolidados na mesma regra/política de firewall;
8. Deve possuir base com objetos de endereço IP, de serviços da internet como Google e Office 365, atualizados dinamicamente pela solução.

2.3.1.2.3 - Controle de Aplicações:

1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;
2. Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado a: tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;
3. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, activedirectory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;
4. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas,

tais como Skype e utilização da rede Tor;

5. Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
6. Deve identificar o uso de táticas evasivas via comunicações criptografadas;
7. A atualização da base de assinaturas de aplicações automaticamente;
8. Deve estar apto a limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos;
9. Permitir a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;
10. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
11. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;
12. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;
13. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts chat e bloquear a chamada de vídeo;
14. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;
15. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);
16. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Nível de risco da aplicação;
17. Deve ser possível a criação de grupos estáticos de aplicações

baseados em características das aplicações como: Categoria da aplicação.

2.3.1.2.4 - Prevenção de Ameaças:

1. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;
   Para este item a solução deve suportar o licenciamento futuro com suporte a performance do 2.3.1.1 item 5;
2. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;
3. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
4. As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;
5. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;
6. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes politicas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
7. Deve permitir o bloqueio de vulnerabilidades;
8. Deverá possuir o seguinte mecanismos de inspeção de IPS: Análise de decodificação de protocolo;
9. Deverá possuir os seguintes mecanismo de inspeção de IPS:
   a. Análise para detecção de anomalias de protocolo;
   b. IP Defragmentation;
   c. Remontagem de pacotes TCP;
   d. Bloqueio de pacotes malformados;
10. Ser capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;

11. Detectar e bloquear a origem de portscans;
12. Bloquear ataques efetuados por worms conhecidos;
13. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
14. Possuir assinaturas para bloqueio de ataques de buffer overflow;
15. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
16. Identificar e bloquear comunicação com botnets;
17. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:
    a. O nome da assinatura ou do ataque;
    b. Aplicação;
    c. Usuário;
    d. origem
    e. destino da comunicação;
18. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação;
19. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;
20. Os eventos devem identificar o país de onde partiu a ameaça;
21. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;
22. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;
23. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando: Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc.;
24. Suportar e estar licenciado com proteção contra ataques de dia zero por meio de integração com solução de Sandbox em nuvem, do mesmo fabricante;
25. Mesmo sem o licenciamento deste recurso de Proteção de Ameaças, deve ser possível criar assinaturas de modo manual para tratar a inspeção até a camada 7 do modelo OSI (Aplicação);

2.3.1.2.5 - Filtro de URL:

1. A solução deve suportar o licenciamento futuro, com as seguintes funcionalidades;
   a. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
   b. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local, em modo de proxy transparente e explícito;
   c. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
   d. Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;
   e. Possuir pelo menos 60 categorias de URLs;
   f. Deve possuir a função de exclusão de URLs do bloqueio, por categoria;
   g. Permitir a customização de página de bloqueio;
   h. Permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão Continuar para permitir o usuário continuar acessando o site);
   i. Além do Explicit Web Proxy, suportar proxy Web transparente;

2.3.1.2.6 - Identificação de Usuários:

1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de dados local;
2. Deve possuir integração com Microsoft Active Directory para

identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários;

3. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários ou qualquer tipo de restrição de uso como, mas não limitado à, utilização de sistemas virtuais, segmentos de rede, etc;
4. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários;
5. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em Usuários e Grupos de usuários;
6. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);
7. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;
8. Permitir integração com tokens para autenticação dos usuários, incluindo, mas não limitado a acesso à internet e gerenciamento da solução.

2.3.1.2.7 - QoS e Traffic Shaping:

1. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como Youtube, Ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máxima largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming;
2. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem;

3. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de destino;
4. Suportar a criação de políticas de QoS e Traffic Shaping por usuário e grupo;
5. Suportar a criação de políticas de QoS e Traffic Shaping por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;
6. Suportar a criação de políticas de QoS e Traffic Shaping por porta;
7. O QoS deve possibilitar a definição de tráfego com banda garantida;
8. O QoS deve possibilitar a definição de tráfego com banda máxima;
9. O QoS deve possibilitar a definição de fila de prioridade;
10. Suportar marcação de pacotes Diffserv, inclusive por aplicação;
11. Suportar modificação de valores DSCP para o Diffserv;
12. Suportar priorização de tráfego usando informação de Type of Service;
13. Deve suportar QOS (traffic-shapping), em interface agregadas ou redundantes.

2.3.1.2.8 - Filtro de Dados:

1. Permitir a criação de filtros para arquivos e dados pré-definidos;
2. Os arquivos devem ser identificados por extensão e tipo;
3. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc);
4. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
5. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
6. Permitir identificar e, opcionalmente, prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.

2.3.1.2.9 - **Geo Localização:**

1. Suportar a criação de políticas por geo-localização, permitindo o trafego de determinado Pais/Países sejam bloqueados;
2. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
3. Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas.

2.3.1.2.10 - VPN

1. Suportar VPN Site-to-Site e Cliente-To-Site;
2. Suportar IPSec VPN;
3. Suportar SSL VPN;
4. A VPN IPSEc deve suportar Autenticação MD5 e SHA-1;
5. A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;
6. A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);
7. A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);
8. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Palo Alto Networks, Fortinet, SonicWall;
9. Suportar VPN em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6;
10. Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de throubleshooting;
11. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;
12. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
13. Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;
14. Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;

15. Deverá manter uma conexão segura com o portal durante a sessão;
16. O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bit), Windows 8 (32 e 64 bit), Windows 10 (32 e 64 bit) e Mac OS X (v10.10 ou superior);
17. Deve suportar agregação de túneis IPSec;
18. Deve suportar algoritmo de balanceamento do tipo WRR (Weighted Round Robin) em agregação de túneis IPSec;
19. A VPN IPSec deve suportar Forward Error Correction (FEC);
20. Deve suportar TLS 1.2 em VPN SSL.

2.3.1.2.11 - Wireless Controller:

1. Deverá administrar e controlar de maneira centralizada os pontos de acesso wireless do mesmo fabricante da solução ofertada;
2. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos;
3. Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac e que transmitam tráfego IPv4 e IPv6 através do controlador;
4. A solução deverá ser capaz de gerenciar pontos de acesso do tipo indoor e outdoor;
5. O controlador wireless deve permitir ser descoberto automaticamente pelos pontos de acesso através de Broadcast, DHCP e consulta DNS;
6. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário;
7. Permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points;
8. 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 devem ser tunelados até o controlador wireless;

9. Quando tunelado, o tráfego deve ser criptografado através de DTLS ou IPSEC;
10. Deve permitir o gerenciamento de pontos de acesso conectados remotamente através de links WAN. Neste cenário o encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma distribuída (local switching), ou seja, o tráfego deve ser comutado localmente na interface LAN do ponto de acesso e não necessitará de tunelamento até o controlador wireless;
11. Quando o encaminhamento do tráfego for distribuído (local switching) e a autenticação via PSK, caso haja falha na comunicação entre os pontos de acesso e o controlador wireless, os usuários associados devem permanecer associados aos pontos de acesso e ao mesmo SSID. Deve ser possível ainda permitir a conexão de novos usuários à rede wireless;
12. A solução deve permitir definir quais redes serão tuneladas até a controladora e quais redes serão comutadas diretamente pela interface do ponto de acesso;
13. A solução deve suportar recurso de Split-Tunneling de forma que seja possível definir, através das subredes de destino, quais pacotes serão tunelados até a controladora e quais serão comutados locamente na interface do ponto de acesso;
14. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;
15. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado dBm;
16. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso;

17. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como Rogue APs. A mitigação deverá ocorrer de forma automática e baseada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados;
18. A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN;
19. A solução deve detectar os pontos de acesso não autorizados e/ou intrusos através de rádios dedicados para a função de análise ou através de Off-channel/Background scanning. Quando realizada através de Off-channel/Background scanning, a solução deve ser capaz de identificar a utilização do ponto de acesso para, caso necessário, atrasar a análise e desta forma não prejudicar os clientes conectados;
20. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless;
21. A solução deve permitir a adição de controlador redundante operando em N+1. Neste modo, o controlador redundante deve monitorar a disponibilidade e sincronizar as configurações do principal, além de assumir todas as funções em caso de falha do controlador primário. Desta forma, todos os pontos de acesso devem se associar automaticamente ao controlador redundante que passará a ter função de primário de forma temporária;
22. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP;
23. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou

grupos de pontos de acesso que cada domínio será habilitado;

24. A solução deve garantir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários;
25. Deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio;
26. A solução deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;
27. A solução deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;
28. A solução deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;
29. A solução deve implementar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless;
30. A solução deve suportar priorização via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada;
31. A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas;
32. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, Fabricante e sistema operacional do dispositivo, Endereço IP, SSID ao qual está conectado, Ponto de acesso ao qual está conectado, Canal ao qual está conectado, Banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação;
33. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir

automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering;

34. A solução deve permitir a configuração de quais data rates estarão ativos na ferramenta e quais serão desabilitados para as frequências de 2.4 e 5GHz e padrões 802.11a/b/g/n/ac;
35. A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime;
36. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados;
37. A solução deve permitir a configuração do valor de Short Guard Interval para 802.11n e 802.11ac em 5GHz;
38. A solução deve implementar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime alocando porcentagens a serem utilizadas nos SSIDs;
39. A solução deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless. Ao menos os seguintes ataques devem ser identificados:
    a. Ataques de flood contra o protocolo EAPOL (EAPOL Flooding);
    b. Association Flood, Authentication Flood, Broadcast Deauthentication e Spoofed Deauthentication;
    c. ASLEAP;
    d. Null Probe Response / Null SSID Probe Response;
    e. Long Duration;
    f. Ataques contra Wireless Bridges;
    g. Weak WEP;
    h. Invalid MAC OUI."
40. A solução deve implementar mecanismos de proteção para mitigar ataques à infraestrutura wireless. Ao menos ataques de negação de serviço devem ser mitigados pela infraestrutura através do envio de pacotes de deauthentication;
41. A solução deve implementar mecanismos de proteção contra ataques do tipo ARP Poisoning na rede wireless;

42. A solução deve monitorar e classificar o risco das aplicações acessadas pelos clientes wireless;
43. Permitir configurar o bloqueio na comunicação entre os clientes wireless conectados a um determinado SSID;
44. Deve implementar autenticação administrativa através do protocolo RADIUS;
45. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);
46. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3;
47. A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID;
48. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada;
49. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;
50. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações 802.1X;
51. A solução deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;
52. A solução deve implementar recurso para autenticação dos usuários através de página web HTTPS, também conhecido como Captive Portal.
53. A solução deve limitar o acesso dos usuários enquanto estes não informarem as credenciais válidas para acesso à rede;
54. A solução deve permitir a hospedagem do captive portal na memória interna do controlador wireless;
55. A solução deve permitir a customização da página de autenticação, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens;
56. A solução deve permitir a coleta de endereço de e-mail dos

usuários como método de autorização para ingresso à rede;

57. A solução deve permitir que a página de autenticação seja hospedada em servidor externo;
58. A solução deve permitir o cadastramento de contas para usuários visitantes na memória interna. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada;
59. A solução deve garantir que usuários se autentiquem em captive portal que faça uso de endereço IPv6;
60. A solução deve possuir interface gráfica para administração e gerenciamento das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução;
61. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado;
62. A solução deve implementar recurso de DHCP Server (IPv4 e IPv6) para facilitar a configuração de redes visitantes;
63. A solução deve identificar automaticamente o tipo de equipamento e sistema operacional utilizado pelo dispositivo conectado à rede wireless;
64. A solução deve permitir que os usuários sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado;
65. A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados;
66. A solução deve permitir a configuração de rede Mesh entre pontos de acesso indoor e outdoor;
67. A solução deve permitir ser gerenciada através dos protocolos HTTPS e SSH via IPv4 e IPv6;
68. A solução deve permitir o envio dos logs para múltiplos servidores syslog externos;
69. A solução deve permitir ser gerenciada através do protocolo SNMP (v1, v2c e v3), além de emitir notificações através da geração de traps;
70. A solução deve incluir suporte para as RFCs 1213 (MIB II) e RFC 2665 (Ethernet-like MIB);

71. A solução deve permitir a captura de pacotes na rede wireless e exporta-los em arquivos no formato .pcap;
72. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD;
73. A solução deve apresentar graficamente a topologia lógica da rede, representar os elementos da rede gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles;
74. A solução deve implementar o gerenciamento unificado e de forma gráfica para redes WiFi e redes cabeadas;
75. A solução deve permitir a atualização de firmware do controlador wireless mesmo quando conectado remotamente;
76. A solução deve permitir a identificação do firmware utilizado por cada ponto de acesso gerenciado e permitir a atualização individualizada através da interface gráfica;
77. A solução deve possuir ferramentas de diagnósticos e debug;
78. A solução deve suportar comunicação com elementos externos através de APIs;
79. A solução deverá ser compatível e gerenciar os pontos de acesso deste processo/lote;

2.3.1.2.12 - SD-WAN:

1. Deve implementar balanceamento de link por hash do IP de origem;
2. Deve implementar balanceamento de link por hash do IP de origem e destino;
3. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links;
4. Deve implementar balanceamento de link por custo configurado do link;
5. Deve suportar o balanceamento de, no mínimo, 5 links;

6. Deve suportar o balanceamento de links de interfaces físicas, sub-interfaces lógicas de VLAN e túneis IPSec;
7. Deve suportar o balanceamento de links LTE (4G) sem restrições de uso, podendo ser usado em conjunto com outros links e não ser somente o backup para todos os outros links;
8. Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;
9. Deve gerar log de eventos que registrem alterações no estado dos links do SDWAN, monitorados pela checagem de saúde;
10. Deve suportar Zero-Touch Provisioning;
11. Possuir checagem do estado de saúde do Link baseando-se em critérios mínimos de: Latência, Jitter e Perda de Pacotes;
12. Deve ser possível configurar a porcentagem de perda de pacotes e o tempo de latência e jitter, na medição de estado de link. Estes valores serão utilizados pela solução para decidir qual link será utilizado;
13. A solução deve permitir modificar o intervalo de tempo de checagem, em segundos, para cada um dos links;
14. A checagem de estado de saúde deve suportar teste com Ping, HTTP e DNS;
15. A checagem de estado de saúde deve suportar a marcação de pacotes com DSCP, para avaliação mais precisa de links que possuem QoS configurado;
16. As regras de escolha do link SD-WAN devem suportar o reconhecimento de aplicações, grupos de usuários, endereço IP de destino e Protocolo;
17. Deve suportar a configuração de nível mínimo de qualidade (latência, jitter e perda de pacotes) para que determinado link seja escolhido pelo SD-WAN;
18. Deve suportar envio de BGP route-map para BGP neighbors, caso a qualidade mínima de um link não seja detectada pela checagem de saúde do link;

<u>2.3.2 - Item 2 – Roteador Remoto SD-WAN com Wi-fi integrado</u>

2.3.2.1 - Características do Equipamento:

1. Deve suportar, no mínimo, 5 Gbps com a funcionalidade de firewall habilitada para tráfego IPv4 e IPv6;
2. Deve suportar, no mínimo, 1 Gbps de throughput IPS;
3. Deve suportar, no mínimo, 4 Gbps de throughput de VPN IPSec;
4. Deve suportar, no mínimo, 300 Mbps de throughput de VPN SSL ou TLS inspection;
5. Deve suportar, no mínimo, 800 Mbps de throughput de Controle de Aplicação;
6. Deve suportar, no mínimo, 500 Mbps de throughput com as seguintes funcionalidades habilitadas simultaneamente, para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: firewall, controle de aplicação, IPS e antimalware;
7. Suporte a, no mínimo, 500.000 conexões simultâneas;
8. Suporte a, no mínimo, 30.000 novas conexões por segundo;
9. Estar licenciado para, ou suportar sem o uso de licença, 180 túneis de VPN IPSEC Site-to-Site simultâneos;
10. Estar licenciado para, ou suportar sem o uso de licença, 220 túneis de clientes VPN IPSEC simultâneos;
11. Estar licenciado para, ou suportar sem o uso de licença adicional, 180 clientes de VPN SSL simultâneos;
12. Permitir gerenciar ao menos 6 Access Points em modo túnel e 12 em modo bridge;
13. Possuir ao menos 4 interfaces 1Gbps;
14. Estar licenciado e/ou ter incluído sem custo adicional, no mínimo, 2 sistemas virtuais lógicos (Contextos) por appliance;
15. Suporte a, no mínimo, 2 sistemas virtuais lógicos (Contextos) por appliance;
16. Possuir no máximo 1 RU de altura.
17. Considerando que a presente contratação tem o objetivo de dar continuidade ao projeto de modernização da rede iniciado em 2020, para atendimento aos requisitos de compatibilidade e padronização da solução, os equipamentos a serem fornecidos neste item devem ser do fabricante Fortinet, modelo FortiWiFi40F, ou superior.

2.3.2.2 - Requisitos Mínimos de Funcionalidade

2.3.2.2.1 - Características Gerais:

1. A solução deve consistir em plataforma de proteção de rede baseada em appliance com funcionalidades de Next Generation Firewall (NGFW), e console de gerência e monitoração;
2. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;
3. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação;
4. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
5. Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19”, incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;
6. A gestão do equipamento deve ser compatível através da interface de gestão Web no mesmo dispositivo de proteção da rede;
7. Os dispositivos de proteção de rede devem possuir suporte a, no mínimo, 200 VLAN Tags 802.1q;
8. Os dispositivos de proteção de rede devem possuir suporte a agregação de links 802.3ad e LACP;
9. Os dispositivos de proteção de rede devem possuir suporte a Policy based routing ou policy based forwarding;
10. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);
11. Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay;
12. Os dispositivos de proteção de rede devem possuir suporte a DHCP Server;
13. Os dispositivos de proteção de rede devem suportar sFlow;
14. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;

15. Deve suportar NAT dinâmico (Many-to-1);
16. Deve suportar NAT dinâmico (Many-to-Many);
17. Deve suportar NAT estático (1-to-1);
18. Deve suportar NAT estático (Many-to-Many);
19. Deve suportar NAT estático bidirecional 1-to-1;
20. Deve suportar Tradução de porta (PAT);
21. Deve suportar NAT de Origem;
22. Deve suportar NAT de Destino;
23. Deve suportar NAT de Origem e NAT de Destino simultaneamente;
24. Deve poder combinar NAT de origem e NAT de destino na mesma politica
25. Deve implementar Network Prefix Translation (NPTv6) ou NAT66;
26. Deve implementar o protocolo ECMP;
27. Deve permitir monitorar via SNMP falhas de hardware, uso de recursos por número elevado de sessões, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede;
28. Deve ser capaz de enviar logs para sistema de monitoramento externo e ser compatível com o software QRadar, utilizado pelo TRE-PR;
29. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;
30. Deve possuir proteção anti-spoofing;
31. Deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2) para IPv4;
32. Suportar OSPF graceful restart;
33. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
34. Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;
35. Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;
36. Deve suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
37. Suporte a configuração de alta disponibilidade Ativo/Passivo ou Ativo/Ativo: Em modo transparente;

38. Suporte a configuração de alta disponibilidade Ativo/Passivo ou Ativo/Ativo: Em layer 3;
39. Suporte a configuração de alta disponibilidade Ativo/Passivo ou Ativo/Ativo: Em layer 3 e com no mínimo 2 equipamentos no cluster;
40. A configuração em alta disponibilidade deve sincronizar: Sessões;
41. A configuração em alta disponibilidade deve sincronizar: Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede;
42. A configuração em alta disponibilidade deve sincronizar: Associações de Segurança das VPNs;
43. A configuração em alta disponibilidade deve sincronizar: Tabelas FIB;
44. O modo de Alta-Disponibilidade deve possibilitar monitoração de falha de link;
45. Deve possuir suporte à criação de sistemas virtuais no mesmo appliance;
46. Em alta disponibilidade, deve ser possível o uso de clusters virtuais, seja ativo-ativo ou ativo-passivo, permitindo a distribuição de carga entre diferentes contextos;
47. O gerenciamento da solução deve suportar acesso via SSH e interface WEB (HTTPS), incluindo, mas não limitado à, exportar configuração dos sistemas virtuais (contextos) por ambas interfaces;
48. Efetuar controle, inspeção e descriptografia de SSL para tráfego de entrada (Inbound) e Saída (Outbound), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos);
49. A solução deve identificar potenciais vulnerabilidades e destacar as melhores práticas que poderiam ser usadas para melhorar a segurança e o desempenho geral de uma rede;
50. O console de administração deve suportar pelo menos inglês;
51. O console deve suportar o gerenciamento de pontos de acesso wireless;

2.3.2.2.2 - Controle por Política de Firewall:

1. Deverá suportar controles por zona de segurança;
2. Efetuar controles de políticas por porta e protocolo;
3. Efetuar controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;
4. Deve efetuar controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
5. Deve suportar a automação de situações como detecção de equipamentos comprometidos, status do sistema, alterações de configuração, eventos específicos e aplicar uma ação que pode ser notificação, bloqueio de um computador, execução de scripts ou funções em nuvem pública;
6. Deve suportar o padrão de indústria 'syslog' protocol para armanazemento usando o formato Common Event Format (CEF);
7. Deve suportar objetos de endereço IPv4 e IPv6, consolidados na mesma regra/política de firewall
8. Deve possuir base com objetos de endereço IP, de serviços da internet como Google e Office 365, atualizados dinamicamente pela solução;
9. A solução deve oferecer suporte à integração nativa com a solução de sandbox, proteção de email, cache e firewall de aplicativos da Web.

2.3.2.2.3 - Controle de Aplicações:

1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;
2. Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado a: tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

3. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, activedirectory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;
4. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;
5. Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
6. Identificar o uso de táticas evasivas via comunicações criptografadas;
7. Atualizar a base de assinaturas de aplicações automaticamente;
8. Deve estar apto a limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos;
9. Permitir a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;
10. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
11. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;
12. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;
13. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts chat e bloquear a chamada de vídeo;
14. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para

os mesmos;

15. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);
16. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Nível de risco da aplicação;
17. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;
18. Deve ser possível configurar Application Override permitindo selecionar aplicações individualmente.

2.3.2.2.4 - Prevenção de Ameaças:

1. Para este item a solução deve suportar o licenciamento futuro com suporte a performance do 2.3.2.1 item 6;
2. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;
3. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
4. As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;
5. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;
6. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes politicas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
7. Deve permitir o bloqueio de vulnerabilidades;
8. Deve incluir proteção contra ataques de negação de serviços;

9. Deverá possuir o seguinte mecanismos de inspeção de IPS: Análise de decodificação de protocolo;
10. Deverá possuir o seguinte mecanismos de inspeção de IPS: Análise para detecção de anomalias de protocolo;
11. Deverá possuir o seguinte mecanismos de inspeção de IPS: IP Defragmentation;
12. Deverá possuir o seguinte mecanismos de inspeção de IPS: Remontagem de pacotes de TCP;
13. Deverá possuir o seguinte mecanismos de inspeção de IPS: Bloqueio de pacotes malformados;
14. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;
15. Detectar e bloquear a origem de portscans;
16. Bloquear ataques efetuados por worms conhecidos;
17. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
18. Possuir assinaturas para bloqueio de ataques de buffer overflow;
19. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
20. Identificar e bloquear comunicação com botnets;
21. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
22. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação;
23. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;
24. Os eventos devem identificar o país de onde partiu a ameaça;
25. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;
26. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;
27. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall

considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança;

28. Suportar e estar licenciado com proteção contra ataques de dia zero por meio de integração com solução de Sandbox em nuvem, do mesmo fabricante;
29. Mesmo sem o licenciamento deste recurso de Proteção de Ameaças, deve ser possível criar assinaturas de modo manual para tratar a inspeção até a camada 7 do modelo OSI (Aplicação).

2.3.2.2.5 - Filtro de URL:

1. Para este item a solução deve suportar o licenciamento futuro;
2. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
3. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local, em modo de proxy transparente e explícito;
4. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
5. Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;
6. Possuir pelo menos 60 categorias de URLs;
7. Deve possuir a função de exclusão de URLs do bloqueio, por categoria;
8. Permitir a customização de página de bloqueio;
9. Permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão Continuar para permitir o usuário continuar acessando o site);
10. Além do Explicit Web Proxy, suportar proxy Web transparente;
11. Mesmo sem o licenciamento deste recurso, deve ser possível criar

regras de filtro URL de modo manual com suporte a expressões regulares.

2.3.2.2.6 - Identificação de Usuários:

1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de dados local;
2. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários;
3. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários ou qualquer tipo de restrição de uso como, mas não limitado à, utilização de sistemas virtuais, segmentos de rede, etc;
4. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários;
5. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em Usuários e Grupos de usuários;
6. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);
7. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
8. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;

9. Permitir integração com tokens para autenticação dos usuários, incluindo, mas não limitado a acesso a internet e gerenciamento da solução;
10. Prover no mínimo um token nativamente, possibilitando autenticação de duplo fator.

2.3.2.2.7 - QoS e Traffic Shaping:

1. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como Youtube, Ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máxima largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming;
2. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem;
3. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de destino;
4. Suportar a criação de políticas de QoS e Traffic Shaping por usuário e grupo;
5. Suportar a criação de políticas de QoS e Traffic Shaping por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;
6. Suportar a criação de políticas de QoS e Traffic Shaping por porta;
7. O QoS deve possibilitar a definição de tráfego com banda garantida;
8. O QoS deve possibilitar a definição de tráfego com banda máxima;
9. O QoS deve possibilitar a definição de fila de prioridade;
10. Suportar marcação de pacotes Diffserv, inclusive por aplicação;
11. Suportar modificação de valores DSCP para o Diffserv;
12. Suportar priorização de tráfego usando informação de Type of Service;
13. Deve suportar QOS (traffic-shapping), em interface agregadas ou redundantes.

2.3.2.2.8 - **Filtro de Dados:**

1. Permitir a criação de filtros para arquivos e dados pré-definidos;
2. Os arquivos devem ser identificados por extensão e tipo;
3. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc);
4. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
5. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
6. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.

2.3.2.2.9 - Geo Localização:

1. Suportar a criação de políticas por geo-localização, permitindo o trafego de determinado Pais/Países sejam bloqueados;
2. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
3. Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas.

2.3.2.2.10 – VPN:

1. Suportar VPN Site-to-Site e Cliente-To-Site;
2. Suportar IPSec VPN;
3. Suportar SSL VPN;
4. A VPN IPSEc deve suportar Autenticação MD5 e SHA-1;
5. A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;
6. A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);
7. A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced

Encryption Standard);

8. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;
9. Suportar VPN em em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6;
10. Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de throubleshooting;
11. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;
12. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
13. Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;
14. Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;
15. Deverá manter uma conexão segura com o portal durante a sessão;
16. O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bit), Windows 8 (32 e 64 bit), Windows 10 (32 e 64 bit) e Mac OS X (v10.10 ou superior);
17. Deve suportar agregação de túneis IPSec
18. Deve suportar algoritmo de balanceamento do tipo WRR (Weighted Round Robin) em agregação de túneis IPSec
19. A VPN IPSec deve suportar Forward Error Correction (FEC)
20. Deve suportar TLS 1.2 em VPN SSL.

2.3.2.2.11 - Wireless Controller:

1. Deverá administrar e controlar de maneira centralizada os pontos de acesso wireless do mesmo fabricante da solução ofertada;
2. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de

referência deverão ser fornecidos;

3. Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac e que transmitam tráfego IPv4 e IPv6 através do controlador;
4. A solução deverá ser capaz de gerenciar pontos de acesso do tipo indoor e outdoor;
5. O controlador wireless deve permitir ser descoberto automaticamente pelos pontos de acesso através de Broadcast, DHCP e consulta DNS;
6. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário;
7. Permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points;
8. 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 devem ser tunelados até o controlador wireless;
9. Quando tunelado, o tráfego deve ser criptografado através de DTLS ou IPSEC;
10. Deve permitir o gerenciamento de pontos de acesso conectados remotamente através de links WAN. Neste cenário o encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma distribuída (local switching), ou seja, o tráfego deve ser comutado localmente na interface LAN do ponto de acesso e não necessitará de tunelamento até o controlador wireless;
11. Quando o encaminhamento do tráfego for distribuído (local switching) e a autenticação via PSK, caso haja falha na comunicação entre os pontos de acesso e o controlador wireless, os usuários associados devem permanecer associados aos pontos de acesso e ao mesmo SSID. Deve ser possível ainda permitir a

conexão de novos usuários à rede wireless;

12. A solução deve permitir definir quais redes serão tuneladas até a controladora e quais redes serão comutadas diretamente pela interface do ponto de acesso;
13. A solução deve suportar recurso de Split-Tunneling de forma que seja possível definir, através das subredes de destino, quais pacotes serão tunelados até a controladora e quais serão comutados locamente na interface do ponto de acesso;
14. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;
15. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado dBm;
16. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso;
17. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como Rogue APs. A mitigação deverá ocorrer de forma automática e baeada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados;
18. A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN;
19. A solução deve detectar os pontos de acesso não autorizados e/ou intrusos através de rádios dedicados para a função de análise ou através de Off-channel/Background scanning. Quando realizada através de Off-channel/Background scanning, a solução deve ser capaz de identificar a utilização do ponto de acesso para, caso necessário, atrasar a análise e desta forma não prejudicar os

clientes conectados;

20. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexbilidade no design da rede wireless;
21. A solução deve permitir a adição de controlador redundante operando em N+1. Neste modo, o controlador redundante deve monitorar a disponibilidade e sincronizar as configurações do principal, além de assumir todas as funções em caso de falha do controlador primário. Desta forma, todos os pontos de acesso devem se associar automaticamente ao controlador redundante que passará a ter função de primário de forma temporária;
22. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP;
23. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado;
24. A solução deve garantir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários; Deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio;
25. A solução deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;
26. A solução deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;
27. A solução deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão

próximos;

28. A solução deve implementar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless;
29. A solução deve suportar priorização via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada;
30. A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas;
31. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, Fabricante e sistema operacional do dispositivo, Endereço IP, SSID ao qual está conectado, Ponto de acesso ao qual está conectado, Canal ao qual está conectado, Banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação;
32. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering;
33. A solução deve permitir a configuração de quais data rates estarão ativos na ferramenta e quais serão desabilitados para as frequências de 2.4 e 5GHz e padrões 802.11a/b/g/n/ac;
34. A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime;
35. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados;
36. A solução deve permitir a configuração do valor de Short Guard Interval para 802.11n e 802.11ac em 5GHz;
37. A solução deve implementar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime alocando

porcentagens a serem utilizadas nos SSIDs;

38. A solução deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless. Ao menos os seguintes ataques devem ser identificados:
39. Ataques de flood contra o protocolo EAPOL (EAPOL Flooding);
40. Os seguintes ataques de negação de serviço: Association Flood, Authentication Flood, Broadcast Deauthentication e Spoofed Deauthentication;
41. ASLEAP;
42. Null Probe Response / Null SSID Probe Response;
43. Long Duration;
44. Ataques contra Wireless Bridges;
45. Weak WEP;
46. Invalid MAC OUI."
47. A solução deve implementar mecanismos de proteção para mitigar ataques à infraestrutura wireless. Ao menos ataques de negação de serviço devem ser mitigados pela infraestrutura através do envio de pacotes de deauthentication;
48. A solução deve implementar mecanismos de proteção contra ataques do tipo ARP Poisoning na rede wireless;
49. A solução deve monitorar e classificar o risco das aplicações acessadas pelos clientes wireless;
50. Permitir configurar o bloqueio na comunicação entre os clientes wireless conectados a um determinado SSID;
51. Deve implementar autenticação administrativa através do protocolo RADIUS;
52. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);
53. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3;
54. A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID;
55. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada;

56. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;
57. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações 802.1X;
58. A solução deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;
59. A solução deve implementar recurso para autenticação dos usuários através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informarem as credenciais válidas para acesso à rede;
60. A solução deve permitir a hospedagem do captive portal na memória interna do controlador wireless;
61. A solução deve permitir a customização da página de autenticação, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens;
62. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede;
63. A solução deve permitir que a página de autenticação seja hospedada em servidor externo;
64. A solução deve permitir o cadastramento de contas para usuários visitantes na memória interna. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada;
65. A solução deve garantir que usuários se autentiquem em captive portal que faça uso de endereço IPv6;
66. A solução deve possuir interface gráfica para administração e gerenciamento das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução;
67. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado;
68. A solução deve implementar recurso de DHCP Server (IPv4 e IPv6) para facilitar a configuração de redes visitantes;
69. A solução deve identificar automaticamente o tipo de

equipamento e sistema operacional utilizado pelo dispositivo conectado à rede wireless;

70. A solução deve permitir que os usuários sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado;
71. A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados;
72. A solução deve permitir a configuração de rede Mesh entre pontos de acesso indoor e outdoor;
73. A solução deve permitir ser gerenciada através dos protocolos HTTPS e SSH via IPv4 e IPv6;
74. A solução deve permitir o envio dos logs para múltiplos servidores syslog externos;
75. A solução deve permitir ser gerenciada através do protocolo SNMP (v1, v2c e v3), além de emitir notificações através da geração de traps;
76. A solução deve permitir que softwares de gerenciamento realizem consultas diretamente nos pontos de acesso via protocolo SNMP;
77. A solução deve incluir suporte para as RFCs 1213 (MIB II) e RFC 2665 (Ethernet-like MIB);
78. A solução deve permitir a captura de pacotes na rede wireless e exporta-los em arquivos no formato .pcap;
79. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD;
80. A solução deve apresentar graficamente a topologia lógica da rede, representar os elementos da rede gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles;
81. A solução deve implementar o gerenciamento unificado e de forma gráfica para redes WiFi e redes cabeadas;
82. A solução deve permitir a atualização de firmware do controlador

wireless mesmo quando conectado remotamente;

83. A solução deve permitir a identificação do firmware utilizado por cada ponto de acesso gerenciado e permitir a atualização individualizada através da interface gráfica;
84. A solução deve possuir ferramentas de diagnósticos e debug;
85. A solução deve suportar comunicação com elementos externos através de APIs;
86. A solução deverá ser compatível e gerenciar os pontos de acesso deste processo;

2.3.2.2.12 - SD-WAN:

1. Deve implementar balanceamento de link por hash do IP de origem;
2. Deve implementar balanceamento de link por hash do IP de origem e destino;
3. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links.
4. Deve implementar balanceamento de link por custo configurado do link.
5. Deve suportar o balanceamento de, no mínimo, 5 links;
6. Deve suportar o balanceamento de links de interfaces físicas, sub-interfaces lógicas de VLAN e túneis IPSec
7. Deve suportar o balanceamento de links LTE (4G) sem restrições de uso, podendo ser usado em conjunto com outros links e não ser somente o backup para todos os outros links.
8. Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;
9. Deve gerar log de eventos que registrem alterações no estado dos links do SDWAN, monitorados pela checagem de saúde
10. Deve suportar Zero-Touch Provisioning
11. Possuir checagem do estado de saúde do Link baseando-se em critérios mínimos de: Latência, Jitter e Perda de Pacotes
12. Deve ser possível configurar a porcentagem de perda de pacotes e o tempo de latência e jitter, na medição de estado de link. Estes

valores serão utilizados pela solução para decidir qual link será utilizado

13. A solução deve permitir modificar o intervalo de tempo de checagem, em segundos, para cada um dos links.
14. A checagem de estado de saúde deve suportar teste com Ping, HTTP e DNS
15. Suportar UDP Hole Punching em arquitetura ADVPN
16. A checagem de estado de saúde deve suportar a marcação de pacotes com DSCP, para avaliação mais precisa de links que possuem QoE configurado
17. As regras de escolha do link SD-WAN devem suportar o reconhecimento de aplicações, grupos de usuários, endereço IP de destino e Protocolo.
18. Deve suportar a configuração de nível mínimo de qualidade (latência, jitter e perda de pacotes) para que determinado link seja escolhido pelo SD-WAN
19. Deve suportar envio de BGP route-map para BGP neighbors, caso a qualidade mínima de um link não seja detectada pela checagem de saúde do link.

2.3.2.2.13 - Access Point:

1. O equipamento deve possuir uma antena integrada para acesso wi-fi de clientes. Se o equipamento ofertado não possuir esta antena, o atendimento a este item poderá ser composto com a entrega de um equipamento adicional para cada roteador remoto adquirido, conforme especificações do item 3 deste lote;
2. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos;
3. Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac em Wave2;
4. Deve suportar operação nas faixas de frequência de 2.4GHz e 5GHz;
5. Deve suportar MU-MIMO 3x3;
6. Deve possuir antenas externas no equipamento com ganho

mínimo de 5dBi em 2.4GHz e 3.5dBi em 5GHz;

7. Deve suportar uma potência de transmissão de no mínimo 20 dBm;
8. Deve suportar velocidades mínimas de 1300 Mbps em 5GHz e 450 Mbps em 2.4GHz;

2.3.3 - Item 3 – Ponto de Acesso Wi-fi:

1. Deve ser do tipo Indoor;
2. Deverá possuir três rádios, sendo eles:
    a. O primeiro rádio deve suportar Taxa de transmissão de no mínimo 574 Mbps e ser configurável para operar em 2.4GHz;
    b. O segundo rádio deve suportar Taxa de transmissão de no mínimo 1200 Mbps e operar em 5GHz;
    c. O terceiro rádio deverá operar em modo dedicado a escaneamento de radiofrequência 24/7 em 2.4GHz e 5GHz, provendo informações de WIDS, Rogue Scanning, etc;
3. Suportar no mínimo 512 usuários associados nos rádios 1 e 2;
4. Deverá possuir também um Rádio do Tipo BLE, além dos rádios explicitados acima;
5. Implementar as tecnologias 802.11 a/b/g/n/ac-W2/ax;
6. Implementar SU-MIMO 2x2;
7. Implementar 802.11ac Wave2 e 802.11ax (Wi-Fi6);
8. Implementar MU-MIMO;
9. Deve permitir que o terceiro rádio seja utilizado como analisador de espectro;
10. Implementar 802.11ac VHT 20/40/80 MHz;
11. Ter potência máxima de ao menos 23dBm considerando 2.4GHz;
12. Sensibilidade RX de ao menos -86 dBm considerando tráfego em VHT40 para MCS 0;
13. Ter ao menos 3 antenas internas;
14. O ganho das antenas internas em 2.4GHz deve ser ao menos 4 dBi;
15. O ganho das antenas internas em 5GHz deve ser ao menos 5 dBi;
16. Ter 1 antena interna do tipo BLE;
17. A antena do tipo BLE deve possuir potência de ao menos 5 dBm;

18. Deve possuir 2 interfaces de rede operando em velocidades de 10/100/1000Mbps, sendo 1 com capacidade de alimentação do equipamento via PoE (PoE 802.3af);
19. Possuir interface de console;
20. Possuir local para conexão de trava Kensington;
21. Deve suportar temperatura de operação até 40 º C;
22. Implementar TransmitBeamforming (TxBF);
23. Possuir certificado WPA3;
24. Deve permitir sua implementação em modo Bridge, Mesh e Tunel;
25. O Fabricante da solução deve possuir ferramenta própria de controle de acesso à rede (NAC), permitindo que posteriormente sejam implementados serviços como DeviceProfiling, descoberta de rede, Políticas de Controle de Acesso, Micro-Segmentação, EndpointCompliance e autenticação avançada com Agentes.
26. Considerando que a presente contratação tem o objetivo de dar continuidade ao projeto de modernização da rede iniciado em 2020, para atendimento aos requisitos de compatibilidade e padronização da solução, os equipamentos a serem fornecidos neste item devem ser do fabricante Fortinet, modelo FortiAP 231F, ou superior.

2.3.3.1 - Requisitos Mínimos de Funcionalidade

2.3.3.1.1 - **Características Gerais:**

1. Ponto de acesso (AP) que permita acesso dos dispositivos à rede através da wireless (sem fio) e que permita que as suas configurações sejam centralizadas em controlador wireless;
2. Deve suportar modo de operação centralizado, ou seja, sua operação depende do controlador wireless que é responsável por gerenciar as políticas de segurança, qualidade de serviço (QoS) e monitoramento da radiofrequência;
3. Deve acompanhar licença que permita que sejam habilitadas todas as suas funcionalidades;
4. Deve identificar automaticamente o controlador wireless ao qual se conectará;

5. Deve permitir ser gerenciado remotamente através de links WAN;
6. Deve possuir capacidade dual-band com rádios 2.4GHz e 5GHz operando simultaneamente, além de permitir configurações independentes para cada rádio;
7. 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 devem ser tunelados até o controlador wireless;
8. Quando tunelado, o tráfego deve ser criptografado através de DTLS ou IPSEC;
9. Deve permitir o gerenciamento de pontos de acesso conectados remotamente através de links WAN. Neste cenário o encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma distribuída (local switching), ou seja, o tráfego deve ser comutado localmente na interface LAN do ponto de acesso e não necessitará de tunelamento até o controlador wireless;
10. Quando o encaminhamento do tráfego for distribuído (local switching) e a autenticação via PSK, caso haja falha na comunicação entre os pontos de acesso e o controlador wireless, os usuários associados devem permanecer associados aos pontos de acesso e ao mesmo SSID. Deve ser possível ainda permitir a conexão de novos usuários à rede wireless;
11. Em conjunto com o controlador wireless, deve otimizar o desempenho e a cobertura wireless (RF), realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados;
12. Possuir funcionalidade de ajuste de potência automática de forma a estender cobertura no caso de falha de APs vizinhos gerenciados pela mesma controladora;
13. Deve suportar mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como Rogue APs;
14. Em conjunto com o controlador wireless, deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless (wIDS/wIPS);

15. Em conjunto com o controlador wireless, deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede;
16. Em conjunto com o controlador wireless, deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);
17. Em conjunto com o controlador wireless, deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;
18. Deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;
19. Deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;
20. Deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;
21. Deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;
22. Deve implementar o padrão IEEE 802.11e;
23. Deve implementar o padrão IEEE 802.11h;
24. Implementar agregação de pacotes A-MPDU e A-MSDU no Access Point;
25. Implementar LPDC - Low Density Parity Check no Access Point;
26. Implementar (MLD) - Maximum Likelihood Demodulation no Access Point;
27. Implementar Maximum Ratio Combining (MRC) no Access Point;
28. Deve possuir indicadores luminosos (LED) para indicação de status;
29. Deve permitir sua alimentação através de Power Over Ethernet (PoE) conforme os padrões 802.3af ou 802.3at;
30. O ponto de acesso deverá ser compatível e ser gerenciado pelos controladores wireless deste processo;

31. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos;
32. Suportar, através de upgrade de licenciamento, método genérico para integração de dispositivos, usando o recebimento, envio, análise e interpretação de mensagens Syslog;
33. Deve ser fornecido com garantia do tipo NBD para no mínimo 24 meses
34. Deve ser fornecido com kit de montagem para teto, permitindo que o Ponto de Acesso seja instalado em superfícies planas, como tetos;

2.3.4 - Item 4 – Serviço de Instalação

1. A realização dos serviços deve ser planejada de acordo com disponibilidade de ambas as partes. O planejamento anterior ao serviço deverá ser realizado de forma on-site nas dependências da CONTRATANTE;
2. O planejamento dos serviços de instalação deve resultar num documento tipo SOW (em tradução livre, escopo de trabalho). Neste documento devem conter a relação, descrição e quantidades dos produtos fornecidos, descrição da infraestrutura existente e desejada, detalhamento dos serviços que serão executados, premissas do projeto, locais e horários de execução dos serviços, condições de execução dos serviços, pontos de contato da CONTRATADA e CONTRATANTE, cronograma de execução do projeto em etapas, com responsáveis e data e início e fim (se aplicável), relação da documentação a ser entregue ao final da execução dos serviços, responsabilidade da CONTRATADA, plano de gerenciamento de mudanças, itens excluídos no projeto e termo de aceite. Os serviços não poderão ser iniciados antes da apresentação e assinatura de concordância de ambas as partes;

3. Todos os parâmetros a serem configurados deverão ser alinhados entre as partes em reuniões de pré-projeto, devendo a CONTRATADA sugerir as configurações de acordo com normas

técnicas e boas práticas, cabendo à CONTRATANTE a sua aceitação expressa ou recusa nos casos de não atendimento das condições estabelecidas;

4. Após a instalação, a solução deverá ser monitorada de forma remota pelo prazo mínimo de 8 (oito) horas corridas, observando as condições de funcionamento e performance dos equipamentos, sendo possível o troubleshooting em caso de problemas ou não conformidades na operação.

5. Ao final da instalação, deverá ser realizado o repasse de configurações hands-on, de forma remota apresentando as configurações realizadas nos equipamentos pelo prazo mínimo de 8 (oito) horas corridas;

6. Os serviços deverão ser realizados por pessoal técnico experiente e certificado pelo fabricante dos equipamentos. A Contratante solicitará os comprovantes da qualificação profissional do(s) técnico(s) que executará(ão) os serviços (conforme item 10.1.c do edital), sendo direito da mesma a sua aceitação ou exigência de troca de profissional no caso de este não satisfazer às condições supramencionadas;

7. Ao término dos serviços deve ser criado um relatório detalhado contendo todos os itens configurados no projeto (relatório as-built), etapas de execução e toda informação pertinente para posterior continuidade e manutenção da solução instalada, como usuários e endereços de acesso, configurações realizadas e o resumo das configurações dos equipamentos.
   a. Este relatório deve ser enviado com todas as informações em até 15 (quinze)dias após a finalização dos serviços;

8. Somente os roteadores concentradores deverão ser instalados de forma on-site nas dependências da CONTRATANTE os demais poderão ser instalados de forma remota;

9. Nos valores cotados devem estar inclusas todas as despesas com deslocamento, alimentação e estadia para realização dos serviços (onsite) nos locais de presença da CONTRATANTE.

9. Os funcionários da CONTRATADA deverão possuir todo o ferramental necessário ao exercício das suas atividades;

10. A CONTRATADA deverá garantir a confidencialidade das informações, dados e senhas compartilhadas da CONTRATANTE, conforme item 10.1.a do edital;

11. As atividades deverão ser realizadas dentro do horário comercial;

12. A implantação não deverá se limitar somente as configurações aqui destacadas. Quaisquer novas funcionalidades suportadas pelos equipamentos poderão fazer parte do escopo do projeto. Estas informações serão documentadas no termo de abertura do projeto a ser documentado pela CONTRATADA após alinhamento do escopo de trabalho entre CONTRATADA e CONTRATANTE;

14. Durante as atividades realizadas na prestação do serviço, o técnico da CONTRATADA deverá demonstrar à equipe técnica de acompanhamento da CONTRATANTE como instalar e configurar os equipamentos e os softwares fornecidos (instalação assistida).

3 – DA ENTREGA E DO RECEBIMENTO

3.1 - DA ENTREGA DO OBJETO

3.1.1 - Todos os equipamentos entregues devem ser de uma única marca e modelo.

3.1.1.1 - A contratada deverá apresentar os equipamentos acondicionados conforme padrão do fabricante. A embalagem deve garantir a proteção do equipamento durante o transporte e estocagem, bem como conter a identificação do produto e demais informações que facilitem a verificação e manuseio dos mesmos.

3.1.2 - Deverá ser fornecida documentação completa e atualizada (manuais, termos de garantia, etc.), no idioma Português, e em quantidade necessária à instalação e à operação dos equipamentos;

3.1.3 - A Contratada deverá fixar nos equipamentos chapa/etiqueta com número de controle patrimonial, a ser fornecida pelo Tribunal Regional Eleitoral do Paraná juntamente com as instruções para fixação das mesmas.

3.1.4 - DO LOCAL DE ENTREGA: Os equipamentos deverão ser entregues na Seção de Rede deste Tribunal, mediante agendamento pelo telefone 41 - 3330-8628.

3.1.4.1 - A entrega deverá ser feita em dias úteis – segunda a sexta-feira – no horário compreendido entre as 12 e as 19 horas, podendo também ocorrer, caso o TRE julgue necessário, em sábados, domingos e feriado.

3.1.5 – DO PRAZO DE ENTREGA:

a) **Para os itens 01 a 03**: prazo máximo **de 50 (cinquenta) dias corridos contados da assinatura do contrato**, estando incluso no valor contratado quaisquer despesas com frete e demais impostos inerentes à contratação.

b) **Para o item 4:** prazo máximo **de 60 (sessenta) dias corridos contados do recebimento dos equipamentos.**

3.1.5.1 - Não serão aceitas entregas de equipamentos no período de recesso deste TRE, ou seja, entre 19 de dezembro e 7 de janeiro.

3.1.6 - Conforme o Art. 3º, inciso III do Decreto 7174/2010[1], caso o produto seja importado, a Contratada deverá apresentar, no momento da entrega, Guia de Recolhimento de Imposto de Importação sobre os produtos a serem fornecidos, mesmo que seja em nome do seu fornecedor, evitando assim, o fornecimento de produtos com entrada ilegal no país, sob pena de não recebimento do objeto, sem prejuízo das sanções cabíveis.

3.2 – DO RECEBIMENTO

3.2.1 – DO RECEBIMENTO PROVISÓRIO

3.2.1.1 - O recebimento provisório será realizado pela Seção de Rede, no prazo máximo de 01 (um) dia.

3.2.2 – DO RECEBIMENTO TÉCNICO E DEFINITIVO

3.2.2.1 - Comissão Técnica com no mínimo 3 (três) servidores a ser instituída pela Secretaria de Tecnologia da Informação realizará, no prazo máximo de 02 (dois) dias úteis, uma inspeção técnica dos equipamentos adquiridos para verificação da sua integridade física e cumprimento das especificações exigidas no edital e seus anexos;

3.2.2.2 - Para a inspeção técnica, será utilizada a documentação entregue pelo fornecedor e/ou fabricante do equipamento contendo as especificações detalhadas dos itens licitados;

3.2.2.3 - A inspeção técnica poderá ser realizada por amostragem, a critério da Administração. O equipamento que, a qualquer tempo durante a vigência do contrato, apresentar irregularidades ou estiver em desacordo com aquele aprovado durante a análise da amostra deverá ser substituído no prazo de até 05 (cinco) dias úteis, contados do comunicado enviado pelo TRE-PR.

---

[1] Art. 3º, inciso III do Decreto 7.174/2010 – *"Além dos requisitos dispostos na legislação vigente, nas aquisições de bens de informática e automação, o instrumento convocatório deverá conter, obrigatoriamente:*
III – exigência contratual de comprovação da origem dos bens importados oferecidos pelos licitantes e da quitação dos tributos de importação a eles referentes, que deve ser apresentada no momento da entrega do objeto (...)"

3.2.2.4 - Os equipamentos deverão ser entregues em perfeito estado de funcionamento, sem marcas, amassados, arranhões e/ou outros problemas físicos;

3.2.2.5 - O equipamento testado deverá possuir todos os componentes e as mesmas características do equipamento ofertado no edital, sendo aceitos componentes e especificações superiores;

3.2.2.6 - Após a inspeção técnica nos equipamentos e verificando que estes estão em perfeitas condições de funcionamento, Comissão Técnica a ser instituída pela Secretaria de Tecnologia da Informação emitirá(ão) o Atestado de Aceite Técnico e definitivo no prazo máximo informado no item 3.2.2.1.

3.2.3.1 - A Coordenadoria de Infraestrutura receberá e encaminhará a nota fiscal e atestado do bem no prazo máximo de 02 (dois) dias úteis.

3.2.4 - Recebido o objeto, mas constatado qualquer defeito/irregularidade, a Contratada deverá providenciar a substituição no prazo de até 05 (cinco) dias úteis, contados do comunicado do TRE/PR, sem quaisquer ônus.

4 – OBRIGAÇÕES E RESPONSABILIDADES DA CONTRATADA

4.1 – DA SUSTENTABILIDADE

4.1.1 - Os equipamentos a serem entregues devem estar em conformidade com as diretrizes RoHS;

4.1.2 - As unidades do equipamento deverão ser entregues devidamente acondicionadas em embalagens individuais adequadas, que utilizem, preferencialmente, materiais recicláveis, de forma a garantir a máxima proteção durante o transporte e a armazenagem;

4.1.3 - A contratada para o fornecimento dos equipamentos, na qualidade de fabricante, importador, distribuidor ou comerciante, poderá ser solicitada a providenciar o recolhimento e o adequado descarte do lixo tecnológico originário desta aquisição de equipamentos, entendido como aqueles produtos ou componentes eletrônicos em desuso e sujeitos a disposição final, para fins de sua destinação final ambientalmente adequada, conforme a Lei 12.305/2010, artigo 33 caput, inciso VI e seus parágrafos;

4.2 – DOS REQUISITOS DE GARANTIA

4.2.1 – A garantia de funcionamento será pelo período de 24 (vinte e quatro) meses contados a partir do Recebimento Definitivo do componente, sem prejuízo de qualquer política de garantia adicional oferecida pelo fabricante.

4.2.1 – Caso haja garantia adicional oferecida pelo fabricante, a Contratada deverá descrever os seus termos na Proposta Detalhada (anexo II).

4.2.2 - A garantia deve incluir todo e qualquer defeito decorrente de projeto, fabricação, construção, montagem, acondicionamento, transporte ou desgaste prematuro, com a substituição de peças, componentes, ajustes, reparos e correções necessárias, às expensas da contratada;

4.2.3 - O fornecedor não poderá, em hipótese alguma, negar-se a registrar chamadas relacionadas ao equipamento adquirido, ainda que se conclua, ao final, que a solução do incidente não seja de responsabilidade do fornecedor/fabricante;

4.2.4 - O prazo máximo para o primeiro atendimento dos chamados é de 02 (dois) dias úteis, contados a partir da abertura do chamado;

4.2.5 - O prazo máximo para a solução do problema é de 3 (três) dias úteis contados a partir do primeiro atendimento, mesmo incluindo a troca de peças e/ou componentes mecânicos ou eletrônicos;

4.2.6 - Em caso de substituição de peças e/ou componentes eletrônicos ou mecânicos, as peças substitutas deverão ser originais do fabricante e ter especificações iguais ou superiores às substituídas;

4.2.7 - As peças e componentes trocados deverão ser novos – não utilizados ou recondicionados;

4.2.8 - O primeiro atendimento dos chamados técnicos deverá ser presencial e feito nas dependências da sede do Tribunal Regional Eleitoral do Paraná (on site) em Curitiba, de segunda-feira a sexta-feira, no horário das 12h30m às 18h30m, por profissionais especializados:

4.2.8.1 - Quando não for possível a solução do problema no local, sendo necessária a remoção do equipamento, o conserto deverá ser efetivado nas dependências do laboratório da Contratada, ficando a mesma responsável pelo translado dos equipamentos e sua devolução em perfeitas condições de uso;

4.2.9 - A Contratada deverá manter, durante os 24 (vinte e quatro) meses de vigência da garantia, e às suas expensas, central de atendimento para abertura de chamados técnicos pelo menos no horário das nove às dezoito horas, de segunda a sexta-feira. A central deverá ser acionada preferencialmente por e-mail. Será aceita também a disponibilização de canal para abertura de chamados técnicos por meio de serviço web da contratada;

4.2.10 - Na abertura do chamado técnico, a Contratada deverá fornecer um número de registro único para cada chamado;

4.2.11 - Considerar-se-á como recebida a solicitação de abertura do chamado técnico após o envio do e-mail (levando em consideração a data e hora do envio do e-mail) ou da abertura da ocorrência/ordem de serviço no serviço web da contratada (este último deve gerar um protocolo de atendimento com as informações de número da ordem de serviço, descrição do pedido de suporte e data e hora da abertura do chamado técnico);

4.2.12 - A contratada deverá entregar, obrigatoriamente, para o fiscal setorial da contratação ao final de todo atendimento realizado um laudo contendo, no mínimo, as seguintes informações:

a) Data e hora da abertura do chamado;
b) Número de registro do chamado;
c) Número do patrimônio TRE-PR do equipamento envolvido;
d) Número de série do equipamento envolvido;
e) Data e hora da chegada do técnico no local de atendimento para o primeiro atendimento;
f) Data e hora da resolução do problema, se aplicável;

g) Procedimentos realizados;
h) No caso de substituição de peças, a descrição do componente substituído.

4.2.12.1 - A contratada deverá encaminhar para o gestor da garantia técnica, através do e-mail rede@tre-pr.jus.br, no prazo máximo de 24 (vinte e quatro) horas após a realização dos atendimentos, uma cópia do laudo deixado com o fiscal da contratação ao final de cada visita técnica.

4.2.13 - A Contratada deverá encaminhar mensalmente, até o 5º (quinto) dia útil do mês subsequente, relatório de todos os chamados técnicos, atendidos ou não, realizados em sua central de atendimento no mês anterior. O relatório deverá conter, pelo menos, as seguintes informações:

a) Data e hora da abertura dos chamados;
b) Número de registro dos chamados;
c) Número do patrimônio TRE-PR dos equipamentos envolvidos;
d) Número de série dos equipamentos envolvidos;
e) Data e hora da chegada do técnico nos locais de atendimento;
f) Data e hora das resoluções dos problemas, quando aplicável;
g) No caso de substituição de peças, a descrição dos componentes substituídos.

4.2.14 - Caso constatado, durante a vigência do contrato, repetidos defeitos em um mesmo componente dentro do lote dos equipamentos adquiridos, principalmente na placa principal, disco rígido ou fonte de alimentação, relacionados à pré-existência de algum vício de conhecimento superveniente à data de sua aquisição, a Contratada será, a critério da Contratante, obrigada a trocar o componente de todos os equipamentos fornecidos;

4.2.15 - A contratada deverá, durante a vigência do contrato, prestar todas as informações solicitadas pelos gestores, esclarecendo dúvidas, inclusive, dando todo o suporte necessário no que tange a levantamentos e estudos referentes ao objeto da contratação, no prazo máximo de 05 (cinco) dias úteis.

4.2.16 - A instituição poderá promover, a qualquer tempo, diligência para checar a veracidade das informações prestadas pela contratada e ainda verificar por amostragem a confrontação do detalhamento das especificações técnicas do Termo de Referência com os equipamentos recebidos.

4.2.16.1 – Constatada alguma irregularidade, a qualquer tempo, a contratada deverá saná-la no prazo máximo de 05 (cinco) dias úteis.

4.3 – OUTRAS OBRIGAÇÕES

4.3.1 – Todos os equipamentos a serem entregues deverão ser idênticos.

4.3.2 - Todas as funcionalidades e/ou licenciamentos descritos para os itens 1, 2 e 3 deste pregão deverão estar licenciados no modelo perpétuo, mantendo as funcionalidades descritas em operação de forma independente da vigência do contrato de garantia dos equipamentos;

4.3.3 - A Contratada fornecedora do equipamento deve garantir que todos os componentes do produto são novos (sem uso, reforma ou recondicionamento) e que não estarão fora de linha de fabricação durante a validade do registro de preço. Será permitida a oferta de equipamentos comprovadamente similares, pelo mesmo preço, no caso de indisponibilidade do originalmente proposto, ficando à critério da contratante o aceite ou não do equipamento ofertado.

4.3.4 - Todos os cabos e conectores externos necessários ao funcionamento dos equipamentos deverão ser fornecidos com comprimento de 1,5m (um metro e cinquenta centímetros). Os cabos de conexão do equipamento à rede elétrica deverão seguir o padrão NBR-14136;

4.3.5 - Para todos os itens de especificação serão aceitas ofertas de qualquer componente de especificação diferente da solicitada, desde que comprovadamente igual ou superior, individualmente, quanto à qualidade, o desempenho, a operacionalidade, a ergonomia ou a facilidade no manuseio do originalmente especificado – conforme o caso, e desde que não cause, direta ou indiretamente, incompatibilidade com qualquer das demais especificações, ou desvantagem nestes mesmos atributos dos demais componentes ofertados.

4.3.6 - É de responsabilidade da Contratada o perfeito fornecimento do objeto, devendo ser de primeira qualidade, obedecendo à garantia legal e às demais normas do Código de Defesa do Consumidor.

4.3.7 - Manter-se em situação de regularidade fiscal durante a contratação, sendo condição necessária para emissão da nota de empenho e para o envio a pagamento.

4.3.8 - Manter atualizados seus endereços de e-mail e telefone junto à Gestão da contratação.

4.3.9 - Manter-se durante toda a execução do contrato em compatibilidade com as obrigações assumidas e todas as condições de habilitação e qualificação exigidas para a contratação até o adimplemento total da contratação.

4.3.10 - Prestar todos os esclarecimentos que forem solicitados pelo TRE PR e atender prontamente às reclamações que lhe forem apresentadas, relacionadas com o fornecimento do objeto contratado.

4.3.11 - Entregar todos os materiais em perfeito estado, sem avarias externas ou defeitos tanto de fabricação como os ocasionados eventualmente no transporte.

4.3.11.1 - A contratada terá seus produtos analisados, no ato do recebimento definitivo e serão recusados aqueles que não satisfizerem as especificações do Termo de Referência.

4.3.12 - São de responsabilidade da Contratada todos os encargos, tributos e despesas necessárias ao transporte e a entrega do objeto em perfeito estado de fornecimento, devendo este ser de primeira qualidade, obedecendo à garantia legal e às demais normas do Código de Defesa do Consumidor.

4.3.13 - Entregar, ao gestor da contratação, em até 5 (cinco) dias úteis após a assinatura do contrato, a declaração constante no anexo III, devidamente preenchida e assinada, conforme item 10.1 do Edital.

5 – DA PROTEÇÃO DE DADOS

5.1 – É vedado às partes a utilização de todo e qualquer dado pessoal repassado em decorrência da execução contratual para finalidade distinta daquela do objeto da contratação, sob pena de responsabilização administrativa, civil e criminal;

5.2 – As partes se comprometem a manter sigilo e confidencialidade de todas as informações – em especial os dados pessoais e os dados pessoas sensíveis – repassados em decorrência da execução contratual, em consonância com o disposto na Lei nº 13.709/2018, sendo vedado o repasse das informações a outras empresas ou pessoas, salvo aquelas decorrentes de obrigações legais ou para viabilizar o cumprimento do edital/instrumento contratual;

5.3 – As partes responderão administrativa e judicialmente, em caso de causarem danos patrimoniais, morais, individual ou coletivo, aos titulares de dados pessoais, repassados em decorrência da execução contratual, por inobservância à LGPD;

5.4 – Em atendimento ao disposto na Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), o CONTRATANTE, para a execução do serviço objeto deste contrato terá acesso aos dados pessoais dos representantes da LICITANTE/CONTRATADA, tais como: número do CPF e do RG, endereço eletrônico, cópia do documento de identificação;

5.5 – A LICITANTE/CONTRATADA/DETENTORA DA ATA declara que tem ciência da existência da Lei Geral de Proteção de Dados (LGPD) e se compromete a adequar todos os procedimentos internos ao disposto na legislação, com intuito de proteção dos dados pessoais repassados pelo CONTRATANTE;

5.6 – A CONTRATADA fica obrigada a comunicar ao CONTRATANTE, em até 24 (vinte e quatro) horas, qualquer incidente de acessos não autorizados aos dados pessoais, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, bem como adotar as providências dispostas no art. 48 da LGPD.

6 – DA GESTÃO DA CONTRATAÇÃO

6.1 - A fiscalização e a gestão serão realizadas por servidores devidamente designados pela Administração, em consonância com o artigo 67, parágrafos 1.º e 2.º: da Lei nº 8.666/93.

6.2 – O Gestor e Fiscais designados para a entrega dos itens licitados deverão anotar em registro próprio todas as ocorrências relacionadas com a execução e determinar o que for necessário à regularização de falhas ou defeitos observados.

7 – DAS DISPOSIÇÕES GERAIS

7.1 - As quantidades previstas no presente Termo de Referência são estimativas máximas para o período de 12 (doze) meses, com entrega conforme cada solicitação, sendo certo que este Tribunal se reserva o direito de adquirir o quantitativo que julgar necessário, podendo ser parcial, integral, ou NÃO adquirir o item.

7.2 - Os licitantes deverão cotar os preços dos bens, seguindo rigorosamente as especificações solicitadas, abstendo-se de cotar aquelas que não puderem atender às condições do edital.

7.3 - Nos valores cotados deverão estar incluídas todas as despesas, tais como fretes, despesas com empregados, equipamentos, veículos, combustíveis, seguros, tributos, dentre outros, que comporão o preço final da proposta do certame.

7.4 - Dúvidas poderão ser sanadas com a Seção de Rede, por meio do telefone (041) 3330-8628 no horário compreendido entre as 12h e as 19h ou pelo e-mail rede@tre-pr.jus.br

Anexo II – Proposta Detalhada

1. A licitante, antes de apresentar sua proposta, DEVERÁ ler atentamente todas as condições deste edital (objeto, obrigações, responsabilidades, etc.), não podendo alegar, depois do certame concluído ou durante a execução do serviço, desconhecimento ou mesmo alegar que cotou erroneamente.

<table>
<tr><td colspan="3"></td></tr>
<tr><td colspan="3">Empresa:
Data:</td></tr>
<tr><th>ITEM</th><th>DISCRIMINAÇÃO</th><th>QUANT.</th></tr>
<tr><td></td><td>(equipamento e modelo)</td><td></td></tr>
<tr><td></td><td>(acessórios)</td><td></td></tr>
<tr><td></td><td>(licenciamento)</td><td></td></tr>
<tr><td></td><td>(sítio da internet para consulta da documentação)</td><td></td></tr>
<tr><td colspan="3">INFORMAR OS TERMOS DE GARANTIA ADICIONAL OFERECIDA PELO FABRICANTE, CASO HAJA. CONFORME ITEM 4.2.1 DO TERMO DE REFERÊNCIA – ANEXO I</td></tr>
<tr><td colspan="3"></td></tr>
<tr><td colspan="3"></td></tr>
<tr><td colspan="3"></td></tr>
<tr><td colspan="3"></td></tr>
</table>

Tribunal Regional Eleitoral
do Paraná

ANEXO III

TERMO DE SIGILO E RESPONSABILIDADE

A empresa ____, neste ato representada por ____, declara que manterá sigilo de qualquer dado ou informação coletada do **Tribunal Regional Eleitoral do Paraná** a que tiver acesso durante o contrato para fornecimento de roteadores para a manutenção da rede redundante do TRE/PR, adotando políticas e boas práticas de segurança da informação, que incluem seus colaboradores diretos, terceirizados, parceiros, fornecedores de software e administradores de serviços de computação em nuvem.

Declara ainda estar ciente da responsabilidade objetiva pelo vazamento ou adulteração de dados, inclusive os de uso pessoal, nos termos da lei.

Nome Completo	**Assinatura**

Cargo ou Função	**Empresa Licitante**

Local	**Data**

Termo de Sigilo e Confidencialidade

Classificação da Informação – Uso Interno

ANEXO IV

TRIBUNAL REGIONAL ELEITORAL DO PARANÁ

ATA DE REGISTRO DE PREÇOS Nº .../2021

O Tribunal Eleitoral do Paraná, situado na Rua João Parolin nº 224 – Prado Velho, Curitiba-PR, inscrito no CNPJ sob o nº 03.985.113/0001-81, neste ato representado por seu Diretor Geral, Dr. Valcir Mombach, nos termos da Lei nº 8.666/93, da Lei nº 10.520/02, dos Decretos nº 10.024/19, nº 7.892/2013 e demais normas legais aplicáveis, em face da classificação da proposta apresentada no Pregão Eletrônico nº xx/2021(PAD 4578/2021), RESOLVE registrar o(s) preço(s) ofertado(s) pelo Fornecedor abaixo:

Empresa:
CNPJ:
Nome do representante legal:
RG nº
CPF nº
Endereço completo:
CEP:
Inscrição Estadual/Municipal:
Telefone:
E-mail:
Banco:
Agência:
Nº Conta Corrente:

Conforme quadro a seguir:

ITEM	DESCRIÇÃO	Unidade	Marca	QTD TRE/PR	PREÇO UNITÁRIO (R$)

1. DO OBJETO

1.1 - A presente Ata tem por objeto o Registro de Preços para **contratação de empresa especializada para fornecimento de solução de comunicação (roteadores, licenças e serviço)**, visando atender às necessidades do Tribunal Regional Eleitoral do Paraná, conforme o edital, as especificações e condições do Termo de Referência e a proposta de preços apresentada, os quais, independentemente de transcrição, fazem parte deste instrumento, naquilo que não o contrarie.

2. DAS OBRIGAÇÕES DAS PARTES

2.1 - Constituem obrigações do **órgão gerenciador**:

a) notificar o fornecedor registrado quanto à requisição do objeto mediante o envio da nota de empenho, a ser repassada via fax ou retirada pessoalmente pelo fornecedor:

a.1) a nota de empenho equivalerá a uma ordem de fornecimento;

b) permitir ao fornecedor o acesso ao local da entrega do objeto, desde que observadas as normas de segurança;

c) notificar o fornecedor de qualquer irregularidade encontrada no fornecimento do objeto;

d) efetuar os pagamentos devidos observadas as condições estabelecidas nesta Ata;

e) promover ampla pesquisa de mercado, de forma a comprovar que os preços registrados permanecem compatíveis com os praticados no mercado.

2.1.1 - Esta Ata não obriga o Tribunal Regional Eleitoral do Paraná a firmar contratações com o fornecedor cujos preços tenham sido registrados, podendo ocorrer licitações específicas para aquisição do objeto desta Ata, observada a legislação pertinente, sendo assegurada preferência de fornecimento ao detentor do registro, em igualdade de condições.

2.2 - Constituem **obrigações do fornecedor**:

a) assinar esta Ata no prazo máximo de 5 (cinco) dias úteis, a contar da convocação.

a) fornecer o objeto conforme especificação e preço registrados;

b) observar as condições estabelecidas no Termo de Referência;

c) entregar o objeto solicitado no prazo máximo definido no item 3.1.5 do anexo I, Termo de Referência.

d) fornecer, sempre que solicitado, no prazo máximo de 5 (cinco) dias, a contar da notificação, documentação de habilitação e qualificação cujas validades encontrem-se vencidas;

e) ressarcir os eventuais prejuízos causados ao órgão gerenciador e participante(s) ou a terceiros, provocados por ineficiência ou irregularidades cometidas na execução das obrigações assumidas;

f) cumprir as demais condições estabelecidas no Termo de Referência – Anexo I.

3. DA VIGÊNCIA DA ATA DE REGISTRO DE PREÇOS

3.1 – Esta Ata de Registro de Preços tem vigência de 12 (doze) meses, contados da data registrada no SIASG.

4. DO GERENCIAMENTO DA ATA DE REGISTRO DE PREÇOS

4.1 - O gerenciamento da Ata de Registro de Preços será feito pela Seção de Rede, determinando o que for necessário à regularização das faltas ou defeitos observados (art. 67 §§ 1º e 2º da Lei nº 8.666/93) e notificará a autoridade superior, quando necessário, para as providências devidas.

4.2 – O fiscal/gestor terá autoridade para exercer toda e qualquer ação de orientação geral e controle junto à Contratada, cabendo ordenar a correção quanto ao fornecimento efetuado em desacordo com as especificações constantes no objeto.

4.3 - O gestor será responsável em comunicar a Contratada, fixando prazos para solucionar problemas, correções dos defeitos ou irregularidades encontradas no fornecimento e/ou prestação dos serviços ora contratados, sob pena de responsabilização administrativa.

4.4 - Se a inexecução persistir, o gestor deverá criar um PAD específico de abertura de processo administrativo e encaminhar à Secretaria de Administração devidamente instruído do comunicado acima e do formulário específico devidamente preenchido, referentes a intenção de abertura de Processo Administrativo.

5. DA VARIAÇÃO DOS PREÇOS REGISTRADOS

5.1 - O reajuste dos preços registrados encontra-se suspenso até disciplinamento diverso oriundo de legislação federal e nas condições desta. Desta forma, os preços permanecerão, em regra, invariáveis pelo período de 01 (um) ano.

5.2 - A atualização monetária somente poderá ocorrer se houver atraso no pagamento motivado pela Administração do TRE.

5.3 - A revisão de preços só será admitida no caso de comprovação do desequilíbrio econômico-financeiro por meio da planilha de custos demonstrativa da majoração e após ampla pesquisa de mercado.

5.3.1 - Para a concessão da revisão dos preços, a(s) empresa(s) deverá(ão) comunicar ao TRE a variação dos preços, por escrito e imediatamente, com pedido justificado de revisão do preço registrado, anexando documentos comprobatórios da majoração e/ou planilha de custos.

5.3.2 - Caso o TRE já tenha emitido a(s) nota(s) de empenho respectiva(s) para que a Contratada realize a entrega dos materiais e a empresa ainda não tenha realizado o pedido de revisão de preços, este não incidirá sobre o(s) pedidos já formalizados e empenhados.

5.4 - O Contratante terá o prazo de 30 (trinta) dias para análise dos pedidos de revisão recebidos.

5.4.1 - Durante esse período a(s) contratada(s) deverão efetuar as entregas dos pedidos pelos preços registrados e nos prazos especificados em cada item, mesmo que a revisão seja julgada procedente pelo TRE. Nesse caso, o TRE procederá ao reforço dos valores pertinentes aos bens empenhados após o pedido de revisão.

5.4.2 - O não cumprimento da entrega nas condições estabelecidas poderá implicar a pena de impedimento do direito de licitar.

5.4.3 - A(s) Contratada(s) obrigar-se-ão em realizar as entregas pelo(s) preço(s) registrado(s) caso o pedido de revisão seja julgado improcedente.

6. DAS SANÇÕES

6.1 - Nos termos da Lei nº 8.666/93 e nº 10.520/02 fica a licitante vencedora sujeita às penalidades previstas no instrumento contratual (Anexo V).

7. DO CANCELAMENTO DA ATA DE REGISTRO DE PREÇOS

7.1 - O registro do fornecedor será cancelado, pelo órgão gerenciador, assegurado o contraditório e a ampla defesa, no prazo de 05 (cinco) dias úteis, a contar do recebimento da notificação, nas seguintes hipóteses:

I. descumprir as condições desta ata de registro de preços bem como do edital e seus anexos;

II. não retirar a nota de empenho ou instrumento equivalente no prazo estabelecido pela Administração, sem justificativa aceitável;

III. não aceitar reduzir o seu preço registrado, na hipótese deste se tornar superior àqueles praticados no mercado;

IV. sofrer sanção prevista nos incisos III ou IV do caput do art. 87 da Lei nº 8.666, de 1993, ou no art. 7º da Lei nº 10.520, de 2002.

7.2 - O cancelamento do registro de preços poderá ocorrer por fato superveniente, decorrente de caso fortuito ou força maior, que prejudique o cumprimento da ata, devidamente comprovados e justificados:

I - por razão de interesse público;

II - a pedido do fornecedor.

7.3 - O cancelamento será precedido de processo administrativo a ser examinado pelo órgão gerenciador, sendo que a decisão final deverá ser fundamentada.

7.4 - A comunicação do cancelamento do registro do fornecedor, nos casos previstos no inciso I do item 7.1, será feito por escrito, juntando-se o comprovante de recebimento.

7.5 - No caso do fornecedor encontrar-se em lugar ignorado, incerto ou inacessível, a comunicação será feita por publicação, no Diário Oficial da União, considerando-se cancelado o registro do fornecedor, a partir do 5º dia útil, a contar da publicação.

7.6 - A solicitação do fornecedor para cancelamento do registro de preço, não o desobriga do fornecimento dos bens/prestação dos serviços até a decisão final do órgão gerenciador, a qual deverá ser prolatada no prazo máximo de 30 (trinta) dias, facultada à Administração a aplicação das penalidades previstas no instrumento convocatório, caso não aceita as razões do pedido.

8. DO FORO

8.1 - Fica eleito o Foro da Comarca de Curitiba-PR. para dirimir as dúvidas oriundas da presente Ata de Registro de Preços.

Curitiba/PR,_____ de ______________ de 2021.

____________________________	____________________________
(Assinatura Representante legal)	Dr. Valcir Mombach
Nome:	Diretor Geral do TRE/PR
CARGO:	

CONTRATO Nº ....../......

PAD nº 4578/2021

ANEXO V

MINUTA DO CONTRATO

CONTRATO DE FORNECIMENTO, INSTALAÇÃO E GARANTIA **que entre si fazem o TRIBUNAL REGIONAL ELEITORAL DO PARANÁ e a empresa ....**

Pelo presente instrumento, regido pela Lei nº 10.520/02, pela Lei nº 8.666/93, suas alterações e demais legislações pertinentes, e em conformidade com o Termo de Abertura de Licitação nº 16/2021, Pregão Eletrônico nº. ..../........., regularmente autorizado pelo ordenador da despesa, PAD 4578/2021, e a proposta vencedora, de um lado o:

TRIBUNAL REGIONAL ELEITORAL DO PARANÁ, inscrito no **CNPJ sob nº. 03.985.113/0001-81,** com sede na Rua João Parolin, nº. 224, Prado Velho, Curitiba/PR, CEP: 80.220-902, telefone: (41) 3330-8500, regularmente autorizado pelo ordenador de despesa, neste ato representado por seu Diretor-Geral, Dr. Valcir Mombach, doravante denominado CONTRATANTE, de outro, a empresa: **...**, inscrita no **CNPJ sob nº. ....**, com sede na Rua ...., nº ...., bairro ...., Cidade/UF ...., CEP: ...., telefone: ...., e-mail: ...., neste ato representada por ...., portador do CPF nº. ...., doravante denominada CONTRATADA, têm entre si ajustado o seguinte:

CLÁUSULA PRIMEIRA: DO OBJETO

1.1 – O presente contrato tem por objeto a **aquisição de Solução de comunicação (roteadores, licenças e serviço),** visando atender às necessidades deste Tribunal Regional Eleitoral.

1.2 - A Contratação obedecerá ao estipulado neste instrumento, bem como às disposições constantes no edital e seus anexos, que, independentemente de transcrição, fazem parte integrante e complementar deste contrato.

1.3 - De acordo com o art. 55 da Lei nº 8.666/93, a prestação dos serviços, objeto deste contrato, será realizada por regime de Empreitada por preço unitário.

CLÁUSULA SEGUNDA: DAS ESPECIFICAÇÕES DO OBJETO

2.1 - O fornecimento, instalação e garantia deverão ser prestados de acordo com o detalhamento previsto no item 2 do Termo de Referência – ANEXO I.

CLÁUSULA TERCEIRA: DA ENTREGA E DO RECEBIMENTO

3.1 – A entrega e o recebimento do objeto ocorrerão conforme o item 3 do Termo de Referência – Anexo I.

CLÁUSULA QUARTA: DAS OBRIGAÇÕES DA CONTRATADA E DA PROTEÇÃO DE DADOS

4.1 – As obrigações da contratada se dará conforme disposições constantes no item 4 do Termo de Referência – Anexo I.

4.2 – A proteção de dados se dará conforme disposições constantes no item 5 do Termo de Referência – Anexo I.

CLÁUSULA QUINTA: DA VIGÊNCIA

5.1 - O presente contrato vigorará pelo período de **26 (vinte e seis) meses,** a partir da data de sua assinatura, **de ...../..../........ a ..../..../........,** , nos termos da Lei nº 8.666/93.

CLÁUSULA SEXTA: DA DESPESA ORÇAMENTÁRIA

6.1 – Os recursos serão destinados à contratação conforme abaixo:

Programa de Trabalho: ....;
Nota de Empenho: 2021NE00.........., emitida em ..../..../2021;
Elemento de Despesa: ....;
Categoria Econômica: ....;
Código SIASG:
Itens 1 e 2: 104620
Item 3: 393277
Item 4: 26972

CLÁUSULA SÉTIMA: DA GESTÃO DA CONTRATAÇÃO

7.1 – Conforme item 6 do Termo de Referência – Anexo I.

CLÁUSULA OITAVA: DO PREÇO E DO PAGAMENTO

8.1 - O valor total do contrato é de **R$.................... (....................)**, a ser pago à CONTRATADA, pelo cumprimento do objeto deste contrato, nos seguintes termos**:**

Item	Descrição	Quantidade	Valor unitário	Valor Total
1	ROTEADOR CONCENTRADOR			

2	**ROTEADOR REMOTO SD-WAN COM WI-FI INTEGRADO**			
3	**PONTO DE ACESSO WI-FI**			
4	**SERVIÇO DE INSTALAÇÃO E SUPORTE**			

8.1.1 – O pagamento total será efetuado após o recebimento definitivo, com envio de nota fiscal ao endereço de e-mail: rede@tre-pr.jus.br e/ou envio da fatura pelo correio.

8.2 – Do documento fiscal:

8.2.1 – O documento fiscal deverá atender os requisitos abaixo, podendo ser emitido na forma eletrônica - NOTA FISCAL ELETRÔNICA, nos termos da legislação vigente, devendo ser encaminhado ao gestor do contrato do TRE/PR, junto a Seção de Rede telefone (041) 3330-8628, pelo e-mail rede@tre-pr.jus.br, em formato PDF ou emitido na forma física devendo ser encaminhado a Seção de Protocolo no horário compreendido entre as 12h e as 19h, localizada na Rua João Parolin, 224, 1º andar, Curitiba/Paraná.

8.2.1.1 – O CNPJ cadastrado no sistema *Comprasnet*, deverá ser o mesmo para efeito de emissão da nota fiscal/fatura para posterior pagamento.

8.2.1.2 - Caso a CONTRATADA não possa emitir a nota fiscal/fatura com o mesmo CNPJ habilitado na licitação, poderá fazê-lo através da eventual matriz ou filial da mesma empresa licitante vencedora. Nesse caso, ambos os CNPJs (licitante vencedora e eventual matriz ou filial utilizada) deverão estar com a documentação fiscal regular.

8.2.1.3 - Outras especificações necessárias às notas fiscais:

- CNPJ da CONTRATADA
- CNPJ do TRE/PR: 03.985.113/0001-81;
- Data de emissão da nota fiscal;
- Descritivo dos valores unitários e totais;
- Número do contrato;
- Banco, agência e número da conta corrente (obrigatoriamente da própria CONTRATADA).

8.3 – Das condições do pagamento:

8.3.1. - O pagamento somente ocorrerá depois de atestado pelo gestor do contrato designado para esta finalidade, à conformidade dos serviços prestados. O atestado será realizado, obedecendo o prazo e formulário específico, conforme dispositivos legais deste TRE/PR.

8.3.2 - O pagamento será efetuado mediante crédito em conta corrente, conforme indicação da contratada no documento fiscal, por intermédio de ordem bancária, de acordo com os seguintes prazos:

8.3.2.1 – Prazo para atestado da Nota fiscal: **até 05 (cinco) dias úteis** a partir do aceite da nota fiscal pelo gestor, a qual deverá ser enviada pela empresa somente após cumpridas todas as exigências contratuais.

8.3.2.1.1 - A Nota Fiscal/Fatura, após o atestado do gestor da contratação, será encaminhada à Secretaria de Orçamento, Finanças e Contabilidade, para que se efetive o pagamento.

8.3.2.2 – Prazo para pagamento da Nota Fiscal: **até 20 (vinte) dias** após o atestado da Nota fiscal pelo Gestor.

8.3.3 – Será considerado como data do pagamento, o dia em que constar como emitida a ordem bancária para pagamento.

8.3.4 - A nota fiscal/fatura apresentada em desacordo com o estabelecido neste Contrato será devolvida à CONTRATADA, e nesse caso, os prazos previstos para o seu atestado e pagamento, serão interrompidos e somente será reiniciada a contagem a partir da respectiva regularização.

8.3.4.1 - Nenhum pagamento será devido à CONTRATADA enquanto pendente de liquidação qualquer obrigação. Este fato não será gerador de direito a reajustamento de preços ou a atualização monetária.

8.3.5 – Havendo erro na apresentação do documento fiscal ou dos documentos pertinentes à contratação, ou ainda, circunstância que impeça a liquidação da despesa, o pagamento ficará pendente até que a CONTRATADA providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a regularização da situação, não acarretando qualquer ônus para o CONTRATANTE.

8.3.6 – Da correção monetária: na eventual atraso de pagamento e, desde que a CONTRATADA não tenha concorrido de alguma forma para tanto, fica convencionado que os encargos moratórios devidos pelo TRE/PR, entre a data prevista para o pagamento e a do efetivo pagamento, mediante solicitação formal da contratada, serão calculados por meio da aplicação da seguinte fórmula: EM = I x N x VP

Onde:
EM = Encargos moratórios;
N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;
VP = Valor da parcela em atraso
I = Índice de compensação financeira = 0,00016438, assim apurado:
I = i/365 (onde i = taxa percentual anual no valor de 6%)
I = (6/100)/365

8.4 – Da regularidade fiscal:

8.4.1 – Todo e qualquer pagamento, decorrente da presente contratação, será precedido de verificação, por parte do TRE/PR, da regularidade fiscal da CONTRATADA em vigor na data do pagamento.

8.4.1.1 – A CONTRATADA inadimplente quanto à regularidade fiscal estará sujeita à abertura de processo administrativo pelo Gestor da contratação do TRE/PR, visando à regularização.

8.4.1.1.1 – Permanecendo a inadimplência poderá haver rescisão contratual, independentemente da aplicação das sanções previstas neste contrato.

CLÁUSULA NONA: DA SUBSTITUIÇÃO TRIBUTÁRIA

9.1 – Da substituição tributária:

9.1.1 - Serão feitas as retenções tributárias federais e municipais incidentes sobre a contratação, conforme artigo 64 da Lei nº 9.430/96, IN RFB 1234/12, IN RFB 971/09, L. C. nº 116/03 e L. C. nº 123/06, conforme o objeto da contratação.

9.2 – Dos tributos federais:

9.2.1 - Será efetuada a retenção dos tributos federais aplicando-se, sobre o valor a ser pago, o percentual constante da Tabela de Retenção da IN RFB 1234/12.

9.2.2 - Quando a empresa for optante do Regime Simplificado Nacional (SIMPLES), não haverá a retenção de que trata o item acima.

9.2.3 - A nota fiscal, cuja empresa CONTRATADA seja Optante do SIMPLES, deverá estar acompanhada da Declaração, nos termos do caput do artigo 6º da IN RFB 1234/12 - anexo IV.

9.3 - Da retenção previdenciária:

9.3.1 - Quando o objeto da contratação contemplar cessão de mão de obra ou empreitada, poderá ocorrer a retenção do INSS prevista no artigo 112, sobre os serviços elencados nos artigos 117 e 118 da IN RFB 971/09.

9.4 - Da retenção do ISS:

9.4.1 - Sobre serviços, poderá ocorrer a retenção do ISS, quando o objeto da contratação se enquadrar no inciso II, do § 2º do art.6º da L. C. nº 116/03.

9.4.2 - Quando a empresa for optante do Regime Simplificado Nacional (SIMPLES), deverá destacar na nota fiscal de prestação de serviços a alíquota na qual está enquadrada, conforme os anexos III ou IV da Lei Complementar nº 123/06. Caso não haja o referido destaque, será considerada a alíquota máxima vigente, ou seja, 5% (cinco por cento).

9.5 - Quanto à incidência das retenções de tributos prevalecerá sempre a legislação vigente, mesmo que venham a contrariar as disposições acima, conforme sua incidência ou não sobre o objeto contratado.

CLÁUSULA DÉCIMA: DO REAJUSTE

10.1 - Os preços não serão reajustáveis, tendo em vista tratar-se de fornecimento e que o prazo de vigência do contrato refere-se ao período de abrangência dos prazos de entrega, instalação, recebimento e garantia contratual.

CLÁUSULA DÉCIMA PRIMEIRA: DAS SANÇÕES ADMINISTRATIVAS

11.1 – O descumprimento de quaisquer das obrigações descritas do presente instrumento poderá ensejar abertura de processo administrativo, garantido o contraditório e a ampla defesa, com aplicação das seguintes sanções, de acordo com o capítulo IV da Lei nº 8.666/93 e artigo 7º da lei nº 10.520/02:

a) Advertência: para faltas leves, não puníveis com multa;

b) Das multas:

b.1) Multa compensatória de 5% (cinco por cento) sobre o valor total do contrato pelo não cumprimento de outras obrigações previstas;

b.2) Multa compensatória de 10% (dez por cento) sobre o valor total do contrato, pelo inadimplemento parcial;

b.3) Multa compensatório de 15% (quinze por cento) sobre o valor total da contratação pela inexecução total do item 04.

b.3) Multa compensatória de 20% (vinte por cento) sobre o valor total do contrato, pelo inadimplemento total, bem como pela cessação da execução contratual.

11.2- A contratada, ao descumprir os prazos previstos para realizar atendimentos, solucionar chamados, entregar o objeto, substituir os componentes defeituosos, entregar relatórios e prestar garantia, estará sujeita às seguintes sanções:

Ação	Descrição	Medidas Corretivas
Deixar de cumprir os prazos previstos para atendimento, conforme previsto nos itens 4.2 do Termo de referência – REQUISITOS DA GARANTIA, por ocorrência	02 (dois) dias úteis de atraso	Advertência
	Superior a 02 (dois) dias úteis de atraso	Multa de 0,05% sobre o valor contratual por dia de atraso
	Superior a 30 (trinta) dias corridos de atraso	Declaração de inadimplemento parcial do contrato - 10% (dez por cento) sobre o valor total do contrato
Deixar de cumprir o prazo previsto para entrega dos equipamentos, conforme itens 3.1.5 e do item 3.1.5.1 do termo de referência	02 (dois) dias úteis de atraso	Advertência
	Superior a 02 (dois) dias úteis de atraso	Multa de 0,5% sobre o valor da parcela não cumprida por dia de atraso
	Superior a 30 (trinta) dias corridos de atraso	Declaração de inadimplemento total do contrato - 20% (vinte por cento) sobre o valor total do contrato
Deixar de cumprir o prazo previsto para substituir equipamentos defeituosos ou irregulares conforme previsto nos itens 4.2.14 e 4.2.15 do termo de referência, por ocorrência	02 (dois) dias úteis de atraso	Advertência
	Superior a 02 (dois) dias úteis de atraso	Multa de 0,1% sobre o valor contratual por dia de atraso
	Superior a 30 (trinta) dias corridos de atraso	Declaração de inadimplemento parcial do contrato - 10% (dez por cento) sobre o valor total do contrato
Deixar de entregar os laudos de atendimentos e os	02 (dois) dias úteis de atraso	Advertência

relatórios, conforme previsto nos itens 4.2.12, 4.2.12.1 e 4.2.13 do termo de referência, por ocorrência	Superior a 02 (dois) dias úteis de atraso	Multa de 0,02% sobre o valor contratual por dia de atraso
	Superior a 30 (trinta) dias corridos de atraso	Declaração de inadimplemento parcial do contrato - 10% (dez por cento) sobre o valor total do contrato

c) **Impedimento de licitar e contratar com a União:** Será aplicada a penalidade de impedimento de licitar e contratar com a União, conforme previsto no art.7º da Lei nº 10.520/02, bem como o descredenciamento do Sicaf, ou dos sistemas de cadastramento de fornecedores a que se refere o inciso XIV do art. 4º da Lei nº 10.520/02, pelo prazo de até 5 (cinco) anos, sem prejuízo das multas previstas em edital e no contrato e das demais cominações legais, conforme a gravidade do inadimplemento da obrigação e quando a empresa, convocada dentro do prazo de validade da sua proposta, não celebrar o contrato, deixar de entregar a documentação exigida ou apresentar documentação falsa para o certame, ensejar o retardamento da execução de seu objeto, não mantiver a proposta, falhar ou fraudar na execução do contrato, comportar-se de modo inidôneo ou cometer fraude fiscal.

11.2 - As multas e os prejuízos causados ao CONTRATANTE serão deduzidos dos valores a serem pagos em favor da CONTRATADA ou, não havendo possibilidade, deverão ser recolhidos em favor da União no prazo máximo de 30 (trinta) dias consecutivos, a contar da data do recebimento da comunicação enviada pelo Tribunal Regional Eleitoral do Paraná.

11.2.1 - Enquanto pendente processo administrativo para aplicação de multa, o Tribunal Regional Eleitoral do Paraná poderá reter parte dos valores previstos em nota fiscal para garantir o adimplemento da penalidade.

11.3 - As multas imputadas à CONTRATADA cujo montante seja superior ao mínimo estabelecido pelo Ministério da Fazenda[1] e não pagas no prazo concedido pela Administração, serão inscritas em Dívida Ativa da União e cobradas com base na Lei nº 6.830/80, sem prejuízo da correção monetária.

11.4 - A CONTRATADA autoriza desde já ao desconto de multa pré-determinada em processo administrativo que garanta a ampla defesa, na primeira fatura a que vier fazer jus.

11.5 - As penalidades serão obrigatoriamente registradas no SICAF.

CLÁUSULA DÉCIMA SEGUNDA: DA RESCISÃO DO CONTRATO

12.1 - Ficará o presente contrato rescindido, a juízo da administração, mediante formalização, assegurado o contraditório e a ampla defesa, nos casos elencados nos arts. 77 e 78 da Lei nº 8.666/93.

12.2 - Será também causa de rescisão se a CONTRATADA alocar funcionários, para o desempenho dos serviços, que sejam cônjuges, companheiros ou parentes em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de ocupantes de cargos de direção e de assessoramento de membros ou juízes vinculados a este Tribunal,

[1] Portaria nº.75 do Ministério da Fazenda, publicada em 22/03/2012 – artigo 1.º, inciso I.

contrariando o artigo 3º da Resolução nº 07, de 18/10/2005, com redação dada pela Resolução nº 09, de 06/12/05, ambas do CNJ (Conselho Nacional de Justiça), nos termos do Anexo IV.

CLÁUSULA DÉCIMA TERCEIRA: DOS CASOS OMISSOS

13.1 – Os casos omissos serão decididos pelo CONTRATANTE, segundo as disposições contidas na Lei nº 8.666/93 e, subsidiariamente, na Lei nº 9.784/99, no Código de Defesa do Consumidor e demais normas e princípios gerais aplicáveis.

CLÁUSULA DÉCIMA QUARTA: DO FORO

14.1 - Fica eleito o foro de Curitiba/PR, com expressa renúncia de qualquer outro, por mais privilegiado que possa vir a ser, para dirimir as divergências oriundas do presente contrato.

14.2 - E, por estarem assim justas e contratadas, assinam o presente em 02 (duas) vias de igual teor e forma.

Curitiba, ... de .... de 2021

...
Representante Legal
P/ CONTRATADA

Dr. Valcir Mombach
Diretor-Geral – TRE-PR.
P/ CONTRATANTE

Juntar os anexos I e III do Edital.