



PODER JUDICIÁRIO FEDERAL  
TRIBUNAL REGIONAL ELEITORAL DO PARANÁ  
SECRETARIA DE GESTÃO ADMINISTRATIVA – COORDENADORIA DE LICITAÇÕES E  
CONTRATOS – SEÇÃO DE LICITAÇÕES

---

LICITAÇÃO N.º 66/2019  
(Pregão Eletrônico - Registro de Preços)  
Protocolo n.º 6279/2019

ABERTURA DA LICITAÇÃO  
DIA 28/11/2019 às 14:00 HORAS

1 – O Tribunal Regional Eleitoral do Paraná (UASG 070019), 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, Lei nº 11.488/2007, pelos Decretos n.º 10.024/2019 e nº 8.538/2015, 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 28 (vinte e oito) de novembro de 2019, às 14:00 horas,** horário de Brasília – DF, no prédio do TRE-PR, sito na Rua João Parolin nº 224, na sala da Comissão Permanente de Licitação, 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](http://www.comprasgovernamentais.gov.br)).

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

## 2 - DO OBJETO

**2.1** - A presente licitação tem como objeto o Registro de Preços para aquisição de solução de proteção de rede com características de Next Generation Firewall (NGFW) para segurança de informação perimetral que inclui filtro de pacotes, controle de aplicação, administração de largura de banda (QoS), VPN IPsec e SSL, IPS, prevenção contra ameaças de vírus, spywares e malwares "Zero Day", Filtro de URL, funcionalidade de Sandbox, bem como controle de transmissão de dados e acesso à Internet, compondo uma plataforma de segurança integrada com garantia e respectiva subscrição por, pelo menos, 36 (trinta e seis) meses, serviços de instalação e treinamento, visando atender às necessidades deste Tribunal Regional Eleitoral, conforme especificações descritas no Termo de Referência - Anexo I.

## 3 - DO CREDENCIAMENTO ESPECÍFICO PARA O 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 (*e-mail* e telefone para contato) rigorosamente atualizados.

**3.2** - Somente poderão participar desta licitação pessoas jurídicas legalmente estabelecidas no País, cujo objeto social expresse 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 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 aplicada 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 nos itens 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** - 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).

**3.7** - 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.

**3.7.1** - 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.

**3.8** - A licitante deverá estar inscrita no sistema eletrônico *Comprasnet*, no site [www.comprasgovernamentais.gov.br](http://www.comprasgovernamentais.gov.br).

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

**3.8.2** - 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.

**3.9** - 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 Tribunal Regional Eleitoral do Paraná responsabilidade por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros.

#### **4 - ENVIO DA PROPOSTA ELETRÔNICA DE PREÇOS<sup>1</sup> 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, **exclusivamente por meio do sistema eletrônico**.

**4.1.1** - As licitantes poderão deixar de apresentar os documentos de habilitação que constem no SICAF.

**4.1.2** - A licitante, no momento do cadastramento da proposta, deverá obrigatoriamente fazer constar a marca do produto, bem como o modelo (referência da linha de fabricação), se houver (no campo da descrição complementar), vez que diversos fabricantes possuem mais de uma linha, com um diferencial de qualidade e especificação da matéria prima utilizada.

---

<sup>1</sup> **Atenção:** 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 quanto ao contrato.

**4.1.3** - A licitante deverá encaminhar, também, as seguintes informações cadastrais através 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** - Os valores máximos unitários estimados para cada um dos itens, que compõem o lote, constam no item 2.2 do Termo de Referência.

**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 no item 2.2 do Termo de Referência.

**4.6** - Os preços propostos deverão ser finais, acrescidos de todas as despesas<sup>2</sup> (fretes, impostos, taxas, etc.) e conter somente duas casas decimais, não sendo admitidos valores simbólicos, irrisórios ou iguais a zero, ensejando a desclassificação.

**4.6.1** - 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.

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

**4.7** - 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 à prestação de serviço descrita neste edital.

**4.8** - 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

<sup>2</sup> Para o caso das cooperativas o valor final deverá contemplar, inclusive, a contribuição Previdenciária (conforme ADI RFB nº 1/2017).

(doze) meses, contados da data registrada no SIASG.

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

**4.10** - Será solicitado, nesta fase, o envio eletrônico das declarações de inexistência de fato superveniente referente à habilitação, de que a empresa não emprega menor, 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 declaração de atendimento aos requisitos legais estabelecidos no art. 3º da Lei Complementar nº 123/06 para a qualificação como microempresa, empresa de pequeno porte ou sociedade cooperativa<sup>3</sup>, se for o caso (conforme item 9.3.1).

**4.11**- As declarações no item 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.

## 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 do registro e valor.

**7.1.1** - Os lances serão ofertados pelos **valores UNITÁRIOS** dos itens, sendo que a desclassificação em qualquer um dos itens implicará a desclassificação da proposta para o respectivo lote.

**7.2** - As licitantes poderão 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\$ 1,00 (um real)** entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta.

<sup>3</sup> art. 34 da Lei nº 11.488/2007.



**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 deverão estar dentro do valor estimado máximo constante neste 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 as licitantes serão informadas, 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, 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 cooperativa, será assegurada preferência de contratação, respeitado o que segue:

- a) A microempresa, empresa de pequeno porte ou cooperativa 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, empresa de pequeno porte ou cooperativa, se habilitada.
- c) Não ocorrendo a contratação da microempresa, empresa de pequeno porte ou cooperativa na forma do sub-item anterior, serão convocadas as demais ME, EPP ou cooperativa 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.
- e) Na hipótese da não-contratação da microempresa, empresa de pequeno porte ou cooperativa nos termos previstos neste Edital, o objeto será adjudicado em favor da proposta originalmente vencedora do certame, desde que sejam atendidos os demais requisitos.

**8.3** - A licitante classificada em primeiro lugar deverá encaminhar, em até 2 (duas) horas, contadas da solicitação do Pregoeiro, a **Proposta Detalhada – Anexo II**, devidamente adequada ao lance final e onde constem discriminados todos os equipamentos que compõem a solução, com os respectivos modelos e softwares necessários, incluindo-a como anexo no sistema *Comprasnet*.

**8.3.1** – A licitante deverá encaminhar o documento constante no item 8.3 devidamente configurado e em formato para impressão.

**8.3.2** – A Proposta Detalhada apresentada deve discriminar todos os equipamentos que compõem a solução, com respectivos modelos e softwares de licenças necessárias;

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

**8.4** - O Pregoeiro efetuará a aceitação, classificando a proposta de **MENOR PREÇO UNITÁRIO DO LOTE**.

**8.4.1** – Não será aceita proposta cujo quantitativo ofertado seja inferior ao estabelecido no item 2.2 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 duas casas decimais**.

**8.5** - A aceitação da proposta classificada ficará vinculada à aprovação da amostra, conforme descrito no item 9 deste edital.

**8.5.1** – Para análise da amostra o certame será suspenso.

**8.5.2** - A não apresentação ou não aprovação da amostra (da licitante classificada em primeiro lugar), independentemente das sanções legais, ensejará sua desclassificação e a convocação da 2ª classificada para a mesma apresentação e assim sucessivamente.

**8.6** - 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 à sua habilitação na ordem de classificação, segundo o critério do **menor valor do lote** e assim, sucessivamente, até a apuração de uma proposta ou lance que atenda ao edital.

**8.6.1** - Ocorrendo a hipótese anterior, o pregoeiro negociará com a licitante, no sentido de se obter preço melhor.

**8.7** – 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.

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

**8.7.2** – 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 AMOSTRA

**9.1** - A licitante com proposta classificada em primeiro lugar deverá apresentar amostra do equipamento ofertado no prazo máximo de **10 (dez) dias corridos**, após o encerramento da etapa de lances, mediante solicitação do Pregoeiro. Este prazo encerra-se às 19h do último dia do prazo aqui estabelecido.

**9.1.1** – Caso fique comprovado, através da análise da proposta detalhada (item 8.3 deste edital), que o equipamento atende a todas as especificações constantes no Termo de Referência – Anexo I, não haverá solicitação de amostra, ficando a licitante, portanto, dispensada de apresentá-la.

**9.2** – A amostra deverá ser encaminhada ao Tribunal Regional Eleitoral do Paraná – Seção de Rede – situado à Rua João Parolin, 224, bairro Prado Velho – Curitiba – PR.

**9.3** - A amostra deverá estar devidamente identificada com o nome da licitante, número do pregão e conter os respectivos prospectos e manuais, se for o caso.

**9.4** - Caso a amostra do primeiro classificado não seja aprovada, será analisada a proposta detalhada do segundo colocado e, se necessário, será solicitada a amostra e assim sucessivamente, até que se obtenha um equipamento que atenda às características e especificações solicitadas no Termo de Referência – Anexo I.



**9.5 - Será rejeitada a amostra que:**

- a) Apresentar divergência em relação às especificações descritas no Termo de Referência – Anexo I;
- b) Apresentar problemas de funcionamento durante a análise técnica.

**9.6 – Será desclassificada a licitante que:**

- a) Não apresentar a amostra, caso seja solicitada;
- b) Apresentar amostra que esteja em desacordo com as especificações constantes no Termo de Referência – Anexo I.
- c) Cuja amostra não seja aprovada no teste efetuado.

**9.7 - As amostras reprovadas deverão ser retiradas das dependências deste TRE, no prazo máximo de 10 (dez) dias corridos, contados a partir da notificação da licitante pelo TRE-PR.**

**9.7.1 - A não retirada das amostras no prazo acima fixado acarretará a requisição do material em favor do Tribunal Regional Eleitoral do Paraná, pela configuração da perda da propriedade, por abandono, de acordo com o artigo 1275 do Código Civil, aplicado subsidiariamente à Lei nº 8.666/93.**

**9.7.2 - O material referido no item anterior será encaminhado para doação, a ser efetuada em conformidade com o Decreto nº 9.373, de 2018, que regulamenta o desfazimento de material no âmbito da Administração Pública Federal.**

**9.8 – As licitantes cujas amostras foram analisadas e aprovadas ficam obrigadas à entrega de produto idêntico ao que foi apresentado como amostra e em conformidade com o descrito em edital, devendo ser novo, de primeira qualidade, e também atender às normas de Defesa do Consumido.**

## **10 - DA HABILITAÇÃO**

**10.1 - 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:**

**10.1.1 - SICAF;**

**10.1.2 - Consulta Consolidada de Pessoa Jurídica - Tribunal de Contas da União (<https://certidoes-apf.apps.tcu.gov.br/>);**

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

**10.2 - 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, Fundo de Garantia por Tempo de Serviço e Justiça do Trabalho, nos termos do artigo 29 da Lei nº 8.666/93, sendo a comprovação desta habilitação obtida *on line* pelo Pregoeiro, que verificará a validade dos documentos.**

**10.2.1 - Caso conste no cadastro do SICAF algum documento**

habilitatório com data de validade expirada, o pregoeiro poderá consultar o(s) documento(s) da licitante vencedora nas páginas (sítios) das entidades responsáveis pelo referido tributo.

**10.2.1.1** – 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<sup>4</sup>.

**10.2.2** - Para as microempresas, empresas de pequeno porte ou sociedades cooperativas, 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. Os documentos originais, comprobatórios da regularização, deverão ser protocolados em até 2 (dois) dias úteis neste Tribunal.

**10.2.2.1** - 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.

**10.2.3** - 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 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 1971.

**10.3** - Além do cadastro no SICAF, exigir-se-á das licitantes:

**10.3.1** - 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

<sup>4</sup> Conforme IN 03/2018 SICAF.

menores de 18 (dezoito) anos e qualquer trabalho a menores de 16 (dezesesseis) anos, salvo na condição de aprendiz, a partir de 14 (quatorze) anos, declaração de atendimento aos requisitos legais para a qualificação como microempresa, empresa de pequeno porte ou sociedade cooperativa<sup>5</sup>, se for o caso, e 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 (tal exigência será feita no momento da elaboração e envio da proposta, por meio eletrônico, conforme item 4.10).

**10.3.2** – Atestado de capacidade técnica, em nome da licitante, expedido por pessoa jurídica de direito público ou privado, que comprove o fornecimento de solução de segurança com características similares às desta contratação (fornecimento de hardware, licenças e serviços especializados).

**10.3.2.1** - Ao TRE/PR será reservado o direito de efetuar diligências a fim de averiguar a veracidade do(os) atestado(s) apresentado(s).

**10.4** - 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

**10.5** - 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.

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

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

## **11 – DOS DOCUMENTOS A SEREM APRESENTADOS APÓS A ASSINATURA DO CONTRATO**

**11.1** – Em até 30 (trinta dias) dias corridos após a assinatura do contrato, deverão ser apresentados, ao gestor da contratação, no momento da entrega dos equipamentos, os documentos elencados no item 3.4 do Termo de Referência – Anexo I.

## **12 – DOS ESCLARECIMENTOS E DA IMPUGNAÇÃO DO ATO CONVOCATÓRIO**

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

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

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

**12.1** - Até 03 (três) dias 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](mailto:cpl@tre-pr.jus.br), sendo necessário que o arquivo seja encaminhado na extensão “.doc”, possibilitando a inserção no sistema *Comprasnet* pelo Pregoeiro.

<sup>5</sup> Art. 34 da Lei nº 11.488/2007

### 13 - DA POSSIBILIDADE DE REDUÇÃO DE PREÇOS E FORMAÇÃO DO CADASTRO DE RESERVA

**13.1** – 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.

**13.1.1** – A convocação para formação do Cadastro de Reserva será feita através de *email*, gerado pelo próprio Sistema *Comprasnet*.

**13.1.2** – 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.

**13.2** - A apresentação de novas propostas na forma do item 13.1 não prejudicará o resultado do certame em relação à licitante melhor classificada.

**13.3** - 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, 9 e 10 deste edital.

### 14 - DA FORMALIZAÇÃO DA ATA DE REGISTRO DE PREÇOS

**14.1** - 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.

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

**14.2** - No caso da licitante vencedora, bem como as licitantes que reduziram seus preços, nos termos do item 13, 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.

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

**14.4** - 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.

**14.5** - 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.

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

## **15 - DA ATA COMPLEMENTAR**

**15.1** - Na hipótese da empresa vencedora ou aquelas que aceitaram reduzir seus preços, após cumprido o contido no item 13.1, 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.

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

## **16 - DA DESPESA ORÇAMENTÁRIA**

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

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

**16.2.1** - 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.

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

## **17 - DO PAGAMENTO**

**17.1** - Conforme especificações constantes na minuta do contrato (Anexo IV).

## **18 - DAS SANÇÕES ADMINISTRATIVAS**

**18.1** – Durante a fase externa da licitação<sup>6</sup>, as licitantes estarão sujeitas 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.”*

**18.2** - 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;

<sup>6</sup> Conforme entendimento firmado pelo TCU, no Acórdão nº 754/2015 – Plenário.



- 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;
- d) Deixar de apresentar a amostra (se solicitada): 04 (quatro) meses.

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

**18.2.2** - 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.

**18.3** - Nos termos da Lei nº 8.666/93 e da Lei nº 10.520/02 fica a licitante vencedora sujeita às penalidades previstas no Instrumento Contratual (anexo IV deste edital).

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

**18.5** - As multas imputadas à Contratada cujo montante seja superior ao mínimo estabelecido pelo Ministério da Economia<sup>7</sup> 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 pelo IGP-M ou outro índice que por ventura venha a substituí-lo.

## 19 - DOS RECURSOS

**19.1** - Das decisões proferidas pelo pregoeiro, caberão recursos nos termos do artigo 44 e parágrafos do Decreto 10.024/2019.

**19.2** - 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 contra-razões 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.

**19.2.1** - Os procedimentos citados no item anterior serão realizados exclusivamente no âmbito do sistema eletrônico.

**19.3** - A falta de manifestação imediata e motivada importará na decadência do direito de recurso e adjudicação do objeto pelo pregoeiro ao vencedor.

**19.4** - O acolhimento de recurso importará a invalidação apenas dos atos insuscetíveis de aproveitamento.

**19.5** - 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

<sup>7</sup>Art. 1º, inc. I, da Portaria n.º 75, do Ministério da Fazenda (atual Ministério da Economia), publicada em 22/03/2012.

**19.1** – Tanto no julgamento das propostas quanto da habilitação, o Pregoeiro poderá sanar erros ou falhas que não alterem a substância das propostas, dos documentos e sua validade jurídica, nos termos do art. 47 do Decreto 10.024/19.

**19.2** - Para efeito de envio de documentos a serem inseridos no sistema *Comprasnet*, considera-se o horário de funcionamento deste Tribunal (12h às 19h).

**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 no 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 pela internet, *home page*: [www.tre-pr.jus.br](http://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:

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

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

Curitiba, 14 de novembro de 2019.

**Julian Velloso Pugh**  
Pregoeiro

## ANEXO I

### TERMO DE REFERÊNCIA

#### 1 – OBJETO

**1.1** – Registro de preço para aquisição de aquisição de solução de proteção de rede com características de *Next Generation Firewall (NGFW)* para segurança de informação perimetral que inclui filtro de pacotes, controle de aplicação, administração de largura de banda (QoS), VPN IPSec e SSL, IPS, prevenção contra ameaças de vírus, *spywares e malwares “Zero Day”*, Filtro de URL, funcionalidade de *Sandbox*, bem como controle de transmissão de dados e acesso à Internet compondo uma plataforma de segurança<sup>1</sup> integrada com garantia e respectiva subscrição por, pelo menos, 36 (trinta e seis) meses, serviços de instalação e treinamento, de acordo com as características e quantitativos constantes neste Termo de Referência.

#### 2 – DAS ESPECIFICAÇÕES E CARACTERÍSTICAS DO OBJETO

**2.1** – Poderão ser adquiridos os itens abaixo informados:

	Item	Descrição	Quantidade	Valor unitário máximo estimado
LOTE 1	1	<i>Appliance Next Generation Firewall (NGFW)</i> , com interface de gerência e respectivas licenças, garantia, suporte e atualizações por 36 meses	02	R\$ 402.916,26
	2	Licenças, garantia, suporte e atualizações por período adicional de 24 meses para toda a solução apresentada no item 1	02	R\$ 256.971,46
	3	Serviços de instalação, configuração e repasse de conhecimento	02	R\$ 41.837,55
	4	Treinamento	06	R\$ 12.994,50

**2.2** - Descrição dos itens e requisitos técnicos mínimos:

##### **2.2.1 – ITEM 1 - *Appliance Firewall NGFW*:**

**2.2.1.1** - Entende-se por “*Appliance Firewall NGFW*”, conjunto formado por *hardware* e respectivas licenças de *software* necessárias para seu funcionamento, incluídas as consoles de gerência e monitoramento.

**2.2.1.1.1** - Para atendimento a esse item será aceito o fornecimento do *hardware* em *appliance* composto por 02 (dois) equipamentos, desde que atendidas todas as características, as funcionalidades e as capacidades descritas neste termo de referência.

**2.2.1.2** - Cada “*Appliance NGFW*” deve possuir as seguintes características, licenciadas para uso:

<sup>1</sup> Por plataforma de segurança entende-se hardware e software integrados do tipo *appliance*

**2.2.1.2.1** - Possuir *throughput* mínimo de 2 Gbps 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, Antivírus e *Anti-spyware*. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será considerado.

**2.2.1.2.2** - Os *throughputs* devem ser comprovados por documento de domínio público do fabricante. A localização destes documentos deve ser informada na proposta detalhada (conforme item 8.3 do edital). A ausência/inexistência de tais documentos resultará desclassificação da proposta.

**2.2.1.2.3** - Os documentos públicos devem comprovar os *throughputs* aferidos com tráfego HTTP ou **blend** de protocolos definidos pelo fabricante como tráfego real (*real-world traffic blend*).

**2.2.1.2.4** - Não será aceita aceleração de pacotes na placa de rede limitando a análise somente até camada 4.

**2.2.1.2.5** - Deve ser capaz de suportar, no mínimo, 1.000.000 conexões simultâneas.

**2.2.1.2.6** - Deve ser capaz de suportar, no mínimo, 55.000 novas conexões por segundo.

**2.2.1.2.7** - Deve ser fornecido com fontes 120/240 AC, redundantes, ou seja, estes elementos devem permitir a sua substituição sem que seja necessário desligar o equipamento.

**2.2.1.2.8** - Deve ser fornecido com *coolers* ou *fans hot-swappable*s, ou seja, estes elementos devem permitir a sua substituição sem que seja necessário desligar o equipamento.

**2.2.1.2.9** - Deve ser fornecido com disco *Solid State Drive* (SSD) com no mínimo 2400 GB.

**2.2.1.2.10** - Deve possuir, no mínimo, 08 (oito) interfaces de rede 10/100/1000 base-TX.

**2.2.1.2.11** - Deve possuir, no mínimo, 04 (quatro) interfaces de rede 10 Gbps SFP+, fornecidos com seus respectivos *transceivers* do tipo SR.

**2.2.1.2.12** - Deve possuir 01 (uma) interface de rede 1 Gbps dedicada para gerenciamento.

**2.2.1.2.13** - Deve possuir 01 (uma) interface do tipo console ou similar.

**2.2.1.2.14** - Deve ser capaz de operar em alta disponibilidade nos modos Ativo/Ativo ou Ativo/Passivo.

**2.2.1.2.15** - Os equipamentos (*appliances*) fornecidos (Alta disponibilidade) devem possuir o mesmo fabricante, modelo e configuração.

**2.2.1.2.16** - Deve suportar, no mínimo, 50 (cinquenta) zonas de segurança.

**2.2.1.2.17** - Deve permitir a expansão futura de, no mínimo, 04 (quatro) instâncias virtuais de *firewall*.

**2.2.1.2.18** - Deve ser fornecido com licenciamento ou suporte sem a necessidade de licença adicional para, no mínimo, 300 (trezentos) clientes de VPN SSL simultâneos.

**2.2.1.2.19** - Deve ser fornecido com licenciamento ou suporte sem a necessidade de licença adicional para, no mínimo, 50 (cinquenta) túneis de VPN IPSEC simultâneos.

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

**2.2.1.4** - Por console de gerência e monitoração, entende-se as licenças de *software* necessárias para as duas funcionalidades.

**2.2.1.5** - A console de gerência e monitoramento não pode residir no mesmo *appliance* de proteção de rede, devendo ser segregadas dos equipamentos dos *appliances* de proteção.

**2.2.1.5.1** - A console de gerência e monitoramento deve ser virtual e deve rodar em ambiente VMWare ESXi 6.0 ou superior.

**2.2.1.6** - Na data da proposta, nenhum dos modelos ofertados poderá estar listado no site do fabricante em como *end-of-life* ou *end-of-sale*.

**2.2.1.7** - Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19", e devem incluir kit tipo trilho para adaptação, se necessário, e cabos de alimentação.

**2.3.1.8** - A solução deve consistir de *appliance* de proteção de rede com funcionalidades de *Next Generation Firewall* (NGFW), e console de gerência e monitoração.

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

**2.2.1.10** - As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos *appliances* desde que obedeçam a todos os requisitos desta especificação.

**2.2.1.11** - A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7.

**2.2.1.12** - O *hardware* e *software* que executem as funcionalidades de proteção de rede, bem como a console de gerência e monitoração, devem ser do tipo *appliance*. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico.

**2.2.1.13** - O *software* deverá ser fornecido em sua versão mais atualizada recomendada pelo fabricante.



**2.2.1.14 -** Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:

- a) Suporte a 1024 VLAN Tags 802.1q
- b) Agregação de links 802.3ad e LACP
- c) Policy based routing ou policy based forwarding
- d) Roteamento multicast (PIM-SM)
- e) DHCP Relay
- f) DHCP Server
- g) Suporte à criação de objetos de rede

**2.2.1.15 -** Suportar sub-interfaces ethernet logicas.

**2.2.1.15.1 -** Suporte a, no mínimo, 10 (dez) roteadores virtuais na mesma instância de *firewall* ou roteamento baseado em políticas (PBR).

**2.2.1.16 -** O *firewall* deve ter a capacidade de testar o funcionamento de rotas estáticas ou rota *default* com a definição de um endereço IP de destino que deve estar comunicável por meio de uma rota. Caso haja falha na comunicação o *firewall* deve ter a capacidade de usar rota alternativa para estabelecer a comunicação.

**2.2.1.17 -** Deve suportar os seguintes tipos de NAT:

- a) Nat dinâmico (*Many-to-1*);
- b) Nat dinâmico (*Many-to-Many*);
- c) Nat estático (1-to-1);
- d) NAT estático (*Many-to-Many*);
- e) Nat estático bidirecional 1-to-1;
- f) Tradução de porta (PAT);
- g) NAT de Origem;
- h) NAT de Destino;
- i) Suportar NAT de Origem e NAT de Destino simultaneamente.

**2.2.1.18 -** Deve implementar o protocolo ECMP.

**2.2.1.19 -** Deve implementar balanceamento de link por pelo menos um dos métodos a seguir: IP de origem, IP de origem e destino ou *round-robin*.

**2.2.1.20 -** Enviar log para sistemas de monitoração externos, simultaneamente.

**2.2.1.21 -** Deve haver a opção de enviar logs para os sistemas de monitoração externos.

**2.2.1.22 -** Proteção de *anti-spoofing*;

**2.2.1.23 -** Dever permitir bloquear conexões que contenham dados no *payload* de pacotes durante o *three-way hand-shake*;

**2.2.1.24 -** Deve exibir nos logs de tráfego o motivo para o término da sessão no *firewall*, incluindo sessões finalizadas onde houver descrição de criptografia de SSL ou SSH.

**2.2.1.25 -** Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2).

**2.2.1.26 -** Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3).

**2.2.1.27 -** Suportar a OSPF *graceful restart*;

**2.2.1.28 -** Deve suportar o protocolo BGP permitindo que o *firewall* possa anunciar rotas para IPv6.

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

**2.2.1.29 -** Os dispositivos de proteção devem ter a capacidade de operar mediante o uso de suas interfaces físicas nos seguintes modos: Modo *sniffer* (monitoramento e análise do tráfego de rede), camada 2 (I2) e camada 3 (I3).

**2.2.1.29.1 -** Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede.

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

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

**2.2.1.30 -** Suporte à configuração de alta disponibilidade Ativo/Passivo ou Ativo/Ativo:

- a) Em modo transparente;
- b) Em layer 3.

**2.2.1.31 -** A configuração em alta disponibilidade deve sincronizar:

- a) Sessões;
- b) Configurações, incluindo, mas não limitado a políticas de *Firewall*, NAT, QOS e objetos de rede;
- c) Associações de Segurança das VPNs;
- d) Tabelas FIB.

**2.2.1.32 -** O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link.

**2.2.1.33 -** As funcionalidades de filtro de pacotes, NAT, VPN IPsec e protocolos de roteamento dinâmico devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de *software* com o fabricante.

#### **2.2.1.34 - Controle por política de *Firewall***

**2.2.1.34.1** - Deverá suportar controles por zona de segurança.

**2.2.1.34.2** - Controles de políticas por porta e protocolo.

**2.2.1.34.3** - Cada regra deve, obrigatoriamente, funcionar nas versões de endereço IP 4 e 6 sem duplicação da base de objetos e regras.

**2.2.1.34.4** - A solução deve identificar de forma automática quais interfaces o tráfego irá ser direcionado, evitando assim que as interfaces de origem e destino tenham que ser obrigatoriamente explicitadas ou obrigatoriamente listadas.

**2.2.1.34.5** - Controle de políticas por aplicações grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações.

**2.2.1.34.6** - Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;

**2.2.1.34.7** - Deve permitir consultar ou criar políticas para objetos das listas externas ou nuvem de inteligência do fabricante a partir da interface de gerência do próprio firewall.

**2.2.1.34.8** - Controle de políticas por código de País (Por exemplo: BR, USA, UK, RUS).

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

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

**2.2.1.34.11** - Deve de-criptografar sites e aplicações que utilizam certificados ECC, incluindo *Elliptical Curve Digital Signature Algorithm (ECDSA)*;

**2.2.1.34.12** - Controle de inspeção e de-criptografia de SSH ou SSL por política.

**2.2.1.34.13** - Bloqueio de, no mínimo, os seguintes tipos de arquivos: cab, msi e exe.

**2.2.1.34.14** - *Traffic shaping* QoS baseado em Políticas (Prioridade, Garantia e Máximo).

**2.2.1.34.15** - Suporte a objetos e regras IPV6.

**2.2.1.34.16** - Suporte a objetos e regras *multicast*.

**2.2.1.34.17** - Deve suportar no mínimo dois dos tipos de negação de tráfego nas políticas de *firewall* a seguir: Drop sem notificação do bloqueio ao usuário, Drop com opção de envio de ICMP *Unreachable* para máquina de origem do tráfego, TCP-Reset para o client, TCP-Reset para o server ou para os dois lados da conexão.

**2.2.1.34.18 -** Suportar a atribuição de agendamento das políticas (ou regras) com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.

#### **2.2.1.35 - Controle de aplicações**

**2.2.1.35.1 -** Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo.

**2.2.1.35.2 -** Deve ser possível efetuar a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos.

**2.2.1.35.3 -** Deve reconhecer nativamente aplicações relacionadas a tráfego *peer-to-peer*, redes sociais, acesso remoto, *update* de *software*, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail.

**2.2.1.35.4 -** Deve reconhecer pelo menos as seguintes aplicações: *bittorrent*, *gnutella*, *skype*, *facebook*, *linked-in*, *twitter*, *citrix*, *logmein*, *teamviewer*, rdp ou ms-rdp, vnc, gmail, *youtube*, *http-tunnel*, *facebook chat*, *gmail chat*, *whatsapp*, *4shared*, *dropbox*, *google drive*, *onedrive*, *db2*, *mysql*, *oracle*, *kerberos*, *ldap*, *radius*, *itunes*, *dhcp*, *ftp*, *dns*, *wins*, *ntp*, *snmp*, *gotomeeting*, *webex*, *evernote* e *google* ou *google-docs*;

**2.2.1.35 -** Deve inspecionar o *payload* de pacote de dados com o objetivo de detectar por meio de expressões regulares assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo. A checagem de assinaturas também deve determinar se uma aplicação está utilizando a porta *default* ou não, incluindo, mas não limitado a RDP na porta 80 ao invés de 3389;

**2.2.1.35.6 -** Deve detectar aplicações por meio de análise comportamental do tráfego observado, incluindo, pelo menos, *Encrypted Bittorrent* e aplicações VOIP.

**2.2.1.35.7 -** 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 ataques mediante a porta 443.

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

**2.2.1.35.9 -** Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado a *Yahoo Instant Messenger* usando HTTP. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do *Webex*. Além de detectar arquivos e outros conteúdos que devem ser inspecionados de acordo as regras de segurança implementadas.

**2.2.1.35.10 -** Deve permitir a utilização de aplicativos para um determinado grupo de usuário e bloquear para o restante, incluindo,

mas não limitado a *Skype*. Deve permitir também a criação de políticas de exceção concedendo o acesso a aplicativos como *Skype* apenas para alguns usuários;

**2.2.1.35.11 -** Deve permitir controle granular para aplicações SaaS, tais como: *Office 365*, *Skype*, aplicativos *google*, *gmail*, etc.;

**2.2.1.35.12 -** Identificar o uso de táticas evasivas via comunicações criptografadas;

**2.2.1.35.13 -** Atualizar a base de assinaturas de aplicações automaticamente.

**2.2.1.35.14 -** Reconhecer aplicações em IPv6.

**2.2.1.35.15 -** Limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD.

**2.2.1.35.16 -** Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente nas estações dos usuários.

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

**2.2.1.35.18 -** Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos: checagem de assinaturas e decodificação de protocolos.

**2.2.1.35.19 -** Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas.

**2.2.1.35.20 -** Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações da instituição.

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

**2.2.1.35.21 -** O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações.

**2.2.1.35.22 -** Deve alertar o usuário quando uma aplicação for bloqueada.

**2.2.1.35.23 -** Deve possibilitar que o controle de portas seja aplicado para todas as aplicações.



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

**2.2.1.35.25 -** Deve possibilitar a diferenciação de tráfegos de *Instant Messaging* (*AIM*, *Gtalk*, *Facebook Chat*, etc.) possuindo granularidade de controle/políticas para os mesmos.

**2.2.1.35.26 -** Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o *Gtalk* chat e bloquear a transferência de arquivos.

**2.2.1.35.27 -** Deve possibilitar a diferenciação de aplicações *Proxies* (*ghostsurf*, *freegate*, etc.) possuindo granularidade de controle/políticas para os mesmos.

**2.2.1.35.28 -** Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como:

- a) Tecnologia utilizada nas aplicações (*Client-Server*, *Browser Based*, *Network Protocol*, etc.);
- b) Nível de risco da aplicação;
- c) Categoria e subcategoria de aplicações;
- d) Aplicações que usem técnicas evasivas, utilizadas por *malwares*, como transferência de arquivos e/ou uso excessivo de banda, etc.

#### **2.2.1.36 - Prevenção de ameaças**

**2.2.1.36.1 -** Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e *Anti-Spyware* (ou *antimalware*) integrados no próprio *appliance* de *Firewall* ou entregue por meio de composição com outro equipamento ou fabricante.

**2.2.1.36.2 -** Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e *Anti-Spyware* ou *antimalware*).

**2.2.1.36.3 -** Deve sincronizar as assinaturas de IPS, Antivírus, *Anti-Spyware* (ou *antimalware*) quando implementado em alta disponibilidade ativo/ativo ou ativo/passivo.

**2.2.1.36.4 -** Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS e *Anti-spyware* ou *antimalware*: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo e enviar *reset* ou *tcp-reset*.

**2.2.1.36.5 -** Deve possuir a capacidade de detectar e prevenir contra ameaças em tráfegos HTTP/2.

**2.2.1.36.6 -** As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração.

**2.2.1.36.7 -** Exceções por IP de origem ou de destino devem ser possíveis nas regras, de forma geral e assinatura a assinatura;

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

**2.2.1.36.9** - Deve permitir o bloqueio de vulnerabilidades.

**2.2.1.36.10** - Deve permitir o bloqueio de *exploits* conhecidos.

**2.2.1.36.11** - Deve incluir proteção contra ataques de negação de serviços.

**2.2.1.36.12** - Deverá possuir os seguintes mecanismos de inspeção de IPS:

- a) Análise de padrões de estado de conexões;
- b) Análise de decodificação de protocolo;
- c) Análise para detecção de anomalias de protocolo;
- d) IP Defragmentation;
- e) Remontagem de pacotes de TCP;
- f) Bloqueio de pacotes malformados.

**2.2.1.36.13** - Ser imune e capaz de impedir ataques básicos como: Synflood, ICMPflood e UDPflood.

**2.2.1.36.14** - Detectar e bloquear a origem de *portscans* com possibilidade de criar exceções para endereços IPs de ferramentas de monitoramento da instituição.

**2.2.1.36.15** - Bloquear ataques efetuados por *worms* conhecidos, permitindo ao administrador acrescentar novos padrões.

**2.2.1.36.16** - Possuir tecnologia ou assinaturas para a mitigação de ataques DoS e DDoS.

**2.2.1.36.17** - Possuir assinaturas para bloqueio de ataques de buffer overflow.

**2.2.1.36.18** - Deverá possibilitar a criação de assinaturas customizadas pelo órgão.

**2.2.1.36.19** - Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS, permitindo a criação de exceções com granularidade nas configurações.

**2.2.1.36.20** - Permitir o bloqueio de vírus e *spywares* (ou *malwares*) em, pelo menos, os seguintes protocolos: HTTP, HTTPS, SMB ou SMB (NetBios-ssn) e SMTP;

**2.2.1.36.20.1** - É permitido uso de *appliance* externo (antivírus de rede), para o bloqueio de vírus e **spywares** em protocolo SMB de forma a conter *malwares* se espalhando horizontalmente pela rede.

**2.2.1.36.21** - Suportar bloqueio de arquivos por tipo.

**2.2.1.36.22 -** Deve estar apto a identificar e bloquear comunicação com botnets.

**2.2.1.36.23 -** Deve suportar várias técnicas de prevenção, incluindo Drop e tcp-rst.

**2.2.1.36.24 -** Registrar na console de monitoração as seguintes informações sobre ameaças identificadas.

**2.2.1.36.24.1 -** O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

**2.2.1.36.25 -** Deve suportar a captura de pacotes (PCAP), por assinatura de IPS e *Anti-spyware*.

**2.2.1.36.26 -** Deve possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos sejam resolvidas pelo Firewall com endereços (IPv4 ou IPv6), previamente definidos.

**2.2.1.36.27 -** Os eventos devem identificar o país de onde partiu a ameaça.

**2.2.1.36.28 -** Proteção contra downloads involuntários usando HTTP de arquivos executáveis maliciosos.

**2.2.1.36.29 -** Rastreamento de vírus em pdf.

**2.2.1.36.30 -** Deve permitir a inspeção em arquivos comprimidos que utilizam o algoritmo *deflate* (zip, gzip, etc.).

**2.2.1.36.31 -** 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.

### **2.3.1.37 - Análise de *malwares***

**2.2.1.37.1 -** Devido aos *Malwares* hoje em dia serem muito dinâmicos e um antivírus comum reativo não ser capaz de detectar os mesmos com a mesma velocidade que suas variações são criadas, a solução ofertada dever possuir funcionalidades para análise de *Malwares* não conhecidos incluídas na própria ferramenta ou entregue com composição com outro fabricante.

**2.2.1.37.2 -** O dispositivo de proteção deve ser capaz de enviar arquivos trafegados de forma automática para análise "*In Cloud*" ou local, onde o arquivo será executado e simulado em ambiente controlado.

**2.2.1.37.3 -** A solução deve ser capaz de selecionar por meio de políticas granulares quais tipos de arquivos sofrerão esta análise incluindo, mas não limitado a: endereço IP de origem/destino, usuário/grupo do AD/LDAP, aplicação, porta, URL/categoria de URL de destino, tipo de arquivo e todas estas opções simultaneamente;

**2.2.1.37.4** - Deve possuir a capacidade de diferenciar arquivos analisados em pelo menos duas das três categorias: malicioso, não malicioso e arquivos não maliciosos, mas com características indesejáveis (como softwares que deixa o sistema operacional lento, que alteram parâmetros do sistema, etc.).

**2.2.1.37.5** - Suportar a análise com pelo menos 50 (cinquenta) tipos de comportamentos maliciosos para a análise da ameaça não conhecida.

**2.2.1.37.6** - Suportar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional *Windows 7* e *Windows 10*;

**2.2.1.37.7** - Deve suportar a monitoração de arquivos trafegados na internet (HTTPs, HTTP e SMTP).

**2.2.1.37.8** - A solução deve possuir a capacidade de analisar em *sandbox links* (http e HTTPs) presentes no corpo de e-mails trafegados em SMTP. Deve ser gerado um relatório caso a abertura do link pela *sandbox* o identifique como site hospedeiro de *exploits*.

**2.2.1.37.9** - Para ameaças trafegadas em protocolo SMTP, a solução deve ter a capacidade de mostrar nos relatórios o remetente, destinatário e assunto dos *e-mails* permitindo identificação ágil do usuário vítima do ataque.

**2.2.1.37.10** - O sistema de análise "*In Cloud*" ou local deve prover informações sobre as ações do *Malware* na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo *Malware*, gerar assinaturas de Antivírus e *Anti-spyware* automaticamente, definir URLs não confiáveis utilizadas pelo novo *Malware* e prover informações sobre o usuário infectado (seu endereço IP e seu login de rede).

**2.2.1.37.11** - Deve permitir o download dos *malwares* identificados a partir da própria interface de gerência.

**2.2.1.37.12** - Deve permitir informar ao fabricante quanto a suspeita de ocorrências de falso-positivo e falso-negativo na análise de *malwares* de dia zero.

**2.2.1.37.13** - Caso a solução de análise de *malware* seja fornecida em *appliance* local, deve possuir, no mínimo, 25 ambientes controlados (*sandbox*) independentes para execução simultânea de arquivos suspeitos.

**2.2.1.37.14** - Caso sejam necessárias licenças de sistemas operacional e softwares para execução de arquivos no ambiente controlado (*sandbox*), as mesmas devem ser fornecidas em sua totalidade, sem custos adicionais para a contratante.

**2.2.1.37.15** - Suportar a análise de arquivos executáveis, ZIP e criptografados em SSL no ambiente controlado.

**2.2.1.37.16 -** Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos Java (.jar), Linux (ELF), RAR e 7-ZIP no ambiente de *sandbox*;

**2.2.1.37.17 -** Permitir o envio de arquivos e links para análise no ambiente controlado de forma automática via API.

### **2.3.1.38- Filtro de URL**

**2.2.1.38.1 -** A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL.

**2.2.1.38.1.1 -** Permite especificar políticas por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

**2.2.1.38.1.2 -** Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs, Redes e Zonas de segurança.

**2.2.1.38.1.3 -** Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs por meio da integração com serviços de diretório, autenticação via ldap, Active Directory, E-directory e base de dados local.

**2.2.1.38.1.4 -** Permitir popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório.

**2.2.1.38.1.5 -** Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL.

**2.2.1.38.1.6 -** Suportar base ou cache de URLs local no *appliance*, evitando **delay** de comunicação/validação das URLs.

**2.2.1.38.1.7 -** Possui pelo menos 50 categorias de URLs.

**2.2.1.38.1.8 -** Deve classificar o nível de risco de URLs ou aplicações em, pelo menos, três níveis: baixo, médio e alto.

**2.2.1.38.1.9 -** A categorização de URL deve analisar toda a URL e não somente até o nível de diretório.

**2.2.1.38.1.10 -** Permitir a criação categorias de URLs customizadas.

**2.2.1.38.1.11 -** Permitir a exclusão de URLs do bloqueio, por categoria.

**2.2.1.38.1.12 -** Permite a customização de página de bloqueio.

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



**2.2.1.38.1.14 -** Suportar a inclusão nos logs do produto de informações das atividades dos usuários.

#### **2.2.1.39- Identificação de usuários**

**2.2.1.39.1 -** Deve ser capaz de criar políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via *Ldap*, *Active Directory* e base de dados local.

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

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

**2.2.1.39.4 -** Deve possuir integração com *LDAP* para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;

**2.2.1.39.4.1 -** Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x ou soluções NAC via *syslog* ou *radius*, para a identificação de endereços IP e usuários.

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

**2.2.1.39.6 -** Suportar a autenticação *Kerberos*.

**2.2.1.39.7 -** Deve suportar autenticação via *Kerberos* para administradores da plataforma de segurança, *Captive Portal* e usuário de VPN SSL;

**2.2.1.39.8 -** 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.

**2.2.1.39.9-** Deve implementar a criação de grupos customizados de usuários no *firewall*, baseado em atributos do LDAP/AD;

**2.2.1.39.10 -** Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em servidores acessados remotamente.

#### **2.2.1.40 - QoS**

**2.2.1.40.1 -** Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como *youtube*, *ustream*, etc.) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo *streaming*.

**2.2.1.40.2 - Suportar a criação de políticas de QoS por:**

- a) Endereço de origem;
- b) Endereço de destino;
- c) Por usuário e grupo do LDAP/AD;
- d) Por aplicações, incluindo, mas não limitado a *Skype, Bittorrent e Youtube*;
- e) Por porta.
- f) O QoS deve possibilitar a definição de limite de *Upload e Download* ou de classes por: banda garantida, banda máxima e fila de prioridade.

**2.2.1.40.3 - Suportar a limitação de upload e download ou a priorização *Real Time* de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype.**

**2.2.1.40.4 - Disponibilizar estatísticas *Real Time* para classes de QoS.**

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

**2.2.1.41 - Filtro de dados**

**2.2.1.41.1 - Permitir a criação de filtros para arquivos e dados pré-definidos.**

**2.2.1.41.2 - Os arquivos devem ser identificados por extensão e assinaturas.**

**2.2.1.41.3 - Permitir a identificação e opcionalmente prevenir a transferência de vários tipos de arquivos (*Office, PDF, etc.*) identificados sobre aplicações (*P2P, Instant Messaging etc.*).**

**2.2.1.41.4 - Suportar identificação de arquivos compactados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos.**

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

**2.2.1.41.6 - Permitir listar o número de aplicações suportadas para controle de dados.**

**2.2.1.41.7 - Permitir listar o número de tipos de arquivos suportados para controle de dados.**

**2.2.1.42 - Geo-localização**

**2.2.1.42.1 - Suportar a criação de políticas por Geo-localização, permitindo que o tráfego de determinado País/Países seja bloqueado.**

**2.2.1.42.2 - Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos.**

**2.2.1.42.3** - Deve possibilitar a criação de regiões geográficas, caso a solução ofertada não possua as regiões pré-cadastradas, e criar políticas utilizando as mesmas para criar políticas utilizando as mesmas.

#### **2.2.1.43 - VPN IPSEC/SSL**

**2.2.1.43.1** - Suportar VPN Site-to-Site e Cliente-To-Site.

**2.2.1.43.2** - Suportar IPSec VPN.

**2.2.1.43.3** - Suportar SSL VPN.

**2.2.1.43.4** - A VPN IPSec deve suportar:

- a) DES e 3DES;
- b) Autenticação MD5 e SHA-1;
- c) *Diffie-Hellman Group 1, Group 2, Group 5 e Group 14*;
- d) Algoritmo *Internet Key Exchange* (IKEv1 e v2);
- e) AES 128 e 256 (*Advanced Encryption Standard*);
- f) Autenticação via certificado IKE PKI.

**2.2.1.43.5** - A VPN SSL deve suportar:

**2.2.1.43.5.1** - O usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB.

**2.2.1.43.5.2** - A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente.

**2.2.1.43.5.3** - Atribuição de endereço IP nos clientes remotos de VPN SSL.

**2.2.1.43.5.4** - Deve permitir a atribuição de IPs fixos nos usuários remotos de VPN SSL.

**2.2.1.43.5.5** - Deve permitir a criação de rotas de acesso e faixas de endereços IP atribuídas a clientes remotos de VPN de forma customizada por usuário.

**2.2.1.43.5.6** - 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*.

**2.2.1.43.5.7** - Atribuição de DNS nos clientes remotos de VPN;

**2.2.1.43.5.8** - Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, *Anti-spyware* (ou *antimalware*) e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL.

**2.2.1.43.5.9** - Suportar autenticação via AD/LDAP, certificado e base de usuários local.

**2.2.1.43.5.10** - Permitir o estabelecimento de túnel VPN *client-to-site* do cliente a plataforma de segurança, integrando-se com as ferramentas de *Windows-logon*.

**2.2.1.43.5.11** - Suportar leitura e verificação de CRL (*certificate revocation list*).

**2.2.1.43.5.12** - O agente de VPN a ser instalado nos equipamentos desktop e laptops, deve ser capaz de ser distribuído de maneira automática via Microsoft SMS, Active Directory ou ser descarregado diretamente desde o seu próprio portal, o qual residirá no centralizador de VPN.

**2.2.1.43.5.13** - O agente deverá comunicar-se com o portal para determinar as políticas de segurança do usuário,

**2.2.1.43.5.14** - Deve permitir que a conexão com a VPN SSL seja estabelecida das seguintes formas:

- a) Após autenticação do usuário na estação;
- b) Sob demanda do usuário.

**2.2.1.43.5.15** - Deve manter uma conexão segura com o portal durante a sessão.

**2.2.1.43.5.16** - O agente de VPN SSL *client-to-site* deve ser compatível com pelo menos: *Windows Vista, Windows 7, Windows 8, Windows 10, Mac OSx, Android e IOS.*

**2.2.1.43.5.17** - Deve possuir a capacidade de identificar se a origem da conexão de VPN é externa ou interna.

**2.2.1.43.5.18** - Deve possuir mecanismos de checagem de conformidade do dispositivo remoto.

**2.2.1.43.5.19** - Para atendimento as funcionalidades de VPN IPSEC/SSL, será permitido a composição com solução de concentrador VPN por meio de *appliance* físico ou virtual desde que a solução proposta seja do mesmo fabricante e não implique em custo ou licença adicional.

#### **2.2.1.44 - Console de gerência e monitoramento**

**2.2.1.44.1** - Deve possuir solução de gerenciamento centralizado, possibilitando o gerenciamento de diversos *appliances*.

**2.2.1.44.2** - O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos *appliances* da plataforma de segurança.

**2.2.1.44.3** - Controle sobre todos os *appliances* da plataforma de segurança em uma única console, com administração de privilégios e funções, salvo o concentrador VPN.

**2.2.1.44.4** - O gerenciamento centralizado deverá ser entregue como *appliance* virtual e deve ser compatível com *VMware ESXi 6.0* ou superior.

**2.2.1.44.5** - Deve permitir controle global de políticas para todos os *appliances* que compõe a plataforma de segurança.

**2.2.1.44.6** - Deve suportar organizar os *appliances* administrados em grupos: os grupos podem ser geográficos, por funcionalidade (por exemplo, IPS), e distribuição.

**2.2.1.44.7** - Deve implementar sistema de hierarquia entre os firewalls gerenciados, onde seja possível aplicar configurações de forma granular em grupos de *firewalls*.

**2.2.1.44.8** - Deve implementar a criação de perfis de usuários com acesso a plataforma de gerenciamento com definição exata de quais informações e de quais *firewalls* e grupos de *firewalls* o usuário terá acesso referente a logs e relatórios.

**2.2.1.44.9** - Deve permitir a criação de objetos.

**2.2.1.44.10** - Deve consolidar logs e relatórios de todos os *appliances* dispositivos administrados.

**2.2.1.44.11** - Deve permitir que exportar backup de configuração automaticamente via agendamento.

**2.2.1.44.12** - Deve permitir que a configuração ou pacote de atualização de versão dos *firewalls* seja importada de forma automática, ou manual, na plataforma de gerenciamento centralizado e que possa ser usada em outros *firewalls* e grupos de *firewalls*.

**2.2.1.44.13** - Deve mostrar os status dos *firewalls* em alta disponibilidade a partir da plataforma de gerenciamento centralizado.

**2.3.1.44.14** - Deve centralizar a administração de regras e políticas do cluster, usando uma única interface de gerenciamento.

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

**2.2.1.44.16** - Deve permitir substituir o certificado de fábrica no acesso HTTPS a gerência do *firewall* como possibilidade de uso de certificado criado localmente na própria solução ou importado de fonte externa.

**2.2.1.44.17** - Caso haja a necessidade de instalação de cliente para administração da solução o mesmo deve ser compatível com sistemas operacionais *Windows*.

**2.2.1.44.18** - O gerenciamento deve permitir/possuir:

- a) Criação e administração de políticas de *firewall* e controle de aplicação;
- b) Criação e administração de políticas de IPS, Antivírus e *Anti-Spyware* ou *Antimalware*;
- c) Criação e administração de políticas de Filtro de URL;
- d) Monitoramento de logs;
- e) Ferramentas de investigação de logs;
- f) Debugging;
- g) Captura de pacotes.

**2.2.1.44.19** - Acesso concorrente de administradores.



**2.2.1.44.20 -** Deve permitir que administradores concorrentes façam modificações, validem e/ou revertam configurações do *firewall* simultaneamente e que cada administrador consiga aplicar apenas as suas alterações de forma independente das realizadas por outro administrador.

**2.2.1.44.21 -** Deve mostrar ao administrador do *firewall* a hora e data do último login e tentativas de login com falha para acessos a partir da interface gráfica e CLI.

**2.2.1.44.22 -** Deve possuir mecanismo busca global na solução onde possa se consultar, por uma *string*, elementos como: nome de objetos, ID ou nome de ameaças, nome de aplicações, nome de políticas e endereços IPs. Permitindo a localização e uso dos mesmos na configuração do dispositivo.

**2.2.1.44.23 -** Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos.

**2.2.1.44.24 -** Deve permitir monitorar via SNMP falhas de hardware e o uso de recursos do equipamento.

**2.2.1.44.25 -** Bloqueio de alterações, no caso acesso simultâneo de dois ou mais administradores.

**2.2.1.44.26 -** Permitir a definição de perfis de acesso à console com permissões granulares como: acesso de escrita e acesso de leitura.

**2.2.1.44.27 -** Efetuar a autenticação integrada ao *Microsoft Active Directory* e servidor *Radius*.

**2.2.1.44.28 -** Permitir efetuar buscas para localizar em quais regras um endereço IP, IP *Range*, *subnet* ou objetos estão sendo utilizados.

**2.2.1.44.29 -** Deve atribuir sequencialmente um número a cada regra de *firewall*, NAT e QoS.

**2.2.1.44.30 -** Permitir a criação de regras que fiquem ativas em horário definido.

**2.2.1.44.31 -** Permitir a criação de regras com data de expiração.

**2.2.1.44.32 -** Efetuar *backup* das configurações e *rollback* de configuração para a última configuração salva.

**2.2.1.44.33 -** Permitir o *Rollback* de Sistema Operacional para a última versão local.

**2.3.1.44.34 -** Permitir o upgrade via SCP ou interface de gerenciamento.

**2.2.1.44.35 -** Permitir a validação regras antes da aplicação.

**2.2.1.44.36 -** Deve implementar mecanismo de validação de configurações antes da aplicação das mesmas permitindo identificar erros.

**2.2.1.44.36.1 -** Caso necessário, será aceito o uso de *appliance* externo para permitir a validação de regras antes da aplicação.

**2.2.1.44.37 -** Deve possibilitar a visualização e comparação de configurações atuais, configuração anterior e configurações antigas.

**2.2.1.44.38 -** Deve possibilitar a integração com a solução de SIEM em uso no TRE-PR, QRadar.

**2.2.1.44.39 -** Deve gerar logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração.

**2.2.1.44.40 -** Deverá ter a capacidade de gerar um relatório gráfico que permita visualizar as mudanças na utilização de aplicações na rede.

**2.2.1.44.41 -** Emitir relatórios em tempo real para a visualização de origens e destinos do tráfego gerado na instituição.

**2.2.1.44.42 -** Deve prover relatórios com visão correlacionada de aplicações, ameaças (IPS, *Antimalware* ou Antivírus e *Anti-spyware*), URLs e filtro de arquivos, para melhor diagnóstico e resposta a incidentes.

**2.2.1.44.43 -** Deve permitir a criação de *Dash-Boards* customizados para visibilidades do tráfego de aplicativos, usuários, categorias de URL, ameaças identificadas pelo IPS, antivírus, *anti-spyware* (ou *anti-malware*), *malwares "Zero Day"* detectados em *sandbox* e tráfego bloqueado.

**2.2.1.44.44 -** O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos dispositivos de segurança.

**2.2.1.44.45 -** Dever permitir a visualização dos *logs* de *malwares* modernos, tráfego (IP de origem, destino, usuário e porta), aplicação, IPS, antivírus, *anti-spyware* (ou *anti-malware*), Filtro de URL e filtro de arquivos.

**2.2.1.44.46 -** Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e *Anti-spyware* ou *Anti-malware*), etc..

**2.2.1.44.47 -** Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus e *Anti-spyware* ou *anti-malware*), e URLs que passaram pela solução.

**2.2.1.44.48 -** Deve possuir mecanismo "*Drill-Down*" para navegação nos relatórios em *Real Time*.

**2.2.1.44.49 -** Nas opções de "*Drill-Down*", ser possível identificar o usuário que fez determinado acesso.

**2.2.1.44.50 -** Deve possuir relatório de visibilidade e uso sobre aplicativos (SaaS). O relatório também deve mostrar os riscos para a segurança do ambiente, tais como a entrega de *malwares* por meio de aplicativos SaaS com a informação do usuário responsável pelo acesso.

**2.2.1.44.51 -** Permitir a rotação dos logs.

**2.2.1.44.52 -** Deve permitir que os logs e relatórios sejam rotacionados automaticamente baseado no tempo em que estão armazenados na solução, assim como no espaço em disco usado.

**2.2.1.44.53 -** Exibição das seguintes informações, de forma histórica e em tempo real:

- a) Situação do dispositivo e do cluster;
- b) Principais aplicações;
- c) Administradores autenticados na gerência da plataforma de segurança;
- d) Status das interfaces;
- e) Uso de CPU;

**2.2.1.44.54 -** No mínimo os seguintes relatórios devem ser gerados:

- a) Resumo gráfico de aplicações utilizadas;
- b) Principais aplicações por utilização de largura de banda de entrada e saída;
- c) Principais aplicações por taxa de transferência de bytes;
- d) Principais hosts por número de ameaças identificadas;
- e) Atividades de um usuário específico do AD/LDAP, incluindo aplicações acessadas, categorias de URL, e ameaças (IPS, Antivírus e *Anti-spyware* ou *anti-malware*), de rede vinculadas a este tráfego;
- f) Deve permitir a criação de relatórios personalizados.

**2.2.1.44.55 -** Gerar alertas automáticos via, pelo menos, por e-mail e SNMP.

**2.2.1.44.56 -** A plataforma de segurança deve permitir através de API (*Application Program Interface*) a integração com sistemas existentes no ambiente da contratante de forma a possibilitar que aplicações desenvolvidas na contratante possam interagir em Real Time com a solução possibilitando assim que regras e políticas de segurança de possam ser modificadas por estas aplicações com a utilização de scripts em linguagens de programação como Perl ou PHP.

**2.2.1.44.57 -** Para comprovação de atendimento aos requisitos técnicos previstos neste termo **não** serão aceitas declarações e/ou cartas de fabricantes ou licitantes. Serão considerados os documentos de domínio público dos respectivos equipamentos e softwares. Caso a documentação de domínio pública seja omissa ou dúbia, poderá ser solicitada amostra para comprovação do atendimento das características (conforme item 9 do edital).

**2.2.1.44.58 -** Os equipamentos ofertados devem obrigatoriamente ter certificação da ANATEL.

**2.2.1.44.59 -** Caso a solução possua licenças relacionadas a armazenamento, deve ser ofertado a de capacidade ilimitada.

**2.2.1.44.60 -** Caso a solução possua módulo de relatórios estendida, deverá ser entregue junto com a solução.

**2.2.1.44.61 -** As licenças de atualização de software (firmware ou drivers) e licenças de atualização de assinaturas deverão ser fornecidas pelo prazo mínimo de 36 (trinta e seis) meses, a contar da data do recebimento definitivo dos produtos, sem ônus adicional para as atualizações e seu uso.

**2.2.1.44.62 -** Garantia de 36 (trinta e seis) meses com envio de peças/equipamentos de reposição em até 3 (três) dias úteis, para todos os componentes da solução.

**2.2.2 – ITEM 2 – Licenças, garantia, suporte e atualizações por período adicional de 24 meses para toda a solução apresentada no item 1:**

**2.2.2.1 -** Este item visa estender, por 24 meses, o funcionamento da solução de proteção de rede com características de Next Generation Firewall (NGFW) e da console de gerência, com todas as garantias de funcionamento do hardware, licenciamentos e respectivas assinaturas de serviço necessárias para seu funcionamento, incluindo, mas não se restringindo a:

**2.2.2.1.1 -** Extensão do prazo de garantia da solução por 24 (vinte e quatro) meses, com envio de peças/equipamentos de reposição em até 3 dias úteis, para todos os componentes da solução;

**2.2.2.1.2 -** Extensão do prazo de uso do serviço de atualização automática da base de classificação e categorização de aplicações conhecidas, sites e URLs, pelo período de 24 (vinte e quatro) meses;

**2.2.2.1.3 -** Extensão do prazo de uso do serviço de atualização automática da base de assinaturas, utilizada pelo serviço de classificação e categorização de arquivos, pelo período de 24 (vinte e quatro) meses;

**2.2.2.1.4 -** Extensão do prazo de atualizações das assinaturas do serviço de classificação e categorização de arquivos, pelo período de 24 (vinte e quatro) meses.

**2.2.3 – ITEM 3 - Serviços de instalação, configuração e repasse de conhecimento.**

**2.2.3.1 -** Os serviços de instalação, configuração e repasse de conhecimento deverão compreender, no mínimo, as seguintes atividades:

- a) Reunião para definição dos requisitos, arquitetura e topologia de instalação;
- b) Instalação física dos appliances em rack;
- c) Energização e conexão dos appliances em rede;
- d) Atualização de firmware dos appliances;
- e) Configuração das interfaces de gerenciamento;
- f) Ativação das licenças adquiridas;
- g) Configuração das interfaces de rede e regras de roteamento;
- h) Configuração dos objetos e regras de firewall e NAT;

- i) Ativação e configuração das funcionalidades de console de gerenciamento, URL Filter, controle de aplicação, VPN, prevenção contra ameaças, antivírus e malwares e sandbox;
- j) Migração de todo o ambiente atual para a nova solução
- k) Acompanhamento do processo de migração para a nova solução;
- l) Elaboração da documentação do ambiente implementado;
- m) Repasse de conhecimento, abordando o funcionamento geral da solução e a utilização da console de gerenciamento, com no mínimo 2 horas de duração.

**2.2.3.2 -** Os serviços devem ser executados de segunda a sexta-feira, das 12 às 19 horas, na sede do TRE-PR.

**2.2.3.3 -** A realização dos serviços deve ser planejada de acordo com disponibilidade de ambas as partes, em prazo máximo de 30 (trinta) dias após a entrega definitiva dos bens ou oficialização da ordem de empenho. O planejamento anterior ao serviço pode ser realizado remotamente através de webconferência ou videoconferência.

**2.2.3.4 -** Ao término dos serviços deve ser criado um relatório detalhado contendo todos os itens configurados no projeto (as-built), etapas de execução e toda informação pertinente a posterior continuidade e manutenção da solução instalada.

**2.2.3.5 -** Durante toda a implantação do projeto, o técnico da contratada deverá demonstrar aos técnicos da contratante como instalar e configurar os equipamentos e os softwares fornecidos (instalação assistida). Esta demonstração deverá contemplar os conceitos das tecnologias utilizadas pelo equipamento e a operação dos principais recursos dos produtos ofertados.

#### **2.2.4 – ITEM 4 - Treinamento**

**2.2.4.1 -** Voucher para treinamento oficial do fabricante, a ser ministrado pelo fabricante ou por um de seus parceiros credenciados.

**2.2.4.2 -** A carga horária mínima do treinamento não poderá ser inferior a 32 (trinta e duas) horas;

**2.2.4.3 -** O treinamento deverá ser realizado no Brasil, em português, contando com aulas teóricas e práticas.

**2.2.4.4 -** O treinamento deve abordar, no mínimo:

- a) Principais funcionalidades;
- b) Configuração inicial;
- c) Configuração de políticas de segurança;
- d) Métodos de integração e autenticação de usuários;
- e) Configurações de NAT e QoS;
- f) Configurações de VPN (IPSec e SSL);
- g) Emissão e personalização de relatórios.

**2.2.4.5 -** Deve ser emitido um certificado para cada servidor que participar da capacitação e tiver frequência mínima de 70% (setenta por cento).

#### **2.2.5 - Do suporte técnico durante a garantia contratual:**



**2.2.5.1-** Durante o período de Garantia, a CONTRATADA deverá prestar suporte técnico, atender às solicitações do TRE-PR, efetuadas pela Seção de Rede, respeitando as condições e níveis de serviço especificados a seguir;

**2.2.5.2-** A severidade dos chamados de suporte e garantia serão determinadas conforme abaixo e o prazo de atendimento será contado a partir da abertura de ordem de serviço e será classificado conforme as severidades especificadas a seguir:

**2.2.5.3-** Severidade ALTA: Esse nível de severidade é aplicado quando há indisponibilidade de componentes da solução ou as aplicações que são acessadas por meio da solução estão indisponíveis.

Dias úteis		Sábados, domingos e feriados	
Prazo de atendimento	Prazo de solução definitiva	Prazo de atendimento	Prazo de solução definitiva
06 (seis) horas	12 (doze) horas	08 (oito) horas	16 (dezesesseis) horas

**2.2.5.4-** Severidade MÉDIA: Esse nível de severidade é aplicado quando há falha no uso da solução, estando ainda disponível, porém apresentando problemas ou instabilidade.

Dias úteis		Sábados, domingos e feriados	
Prazo atendimento	Prazo de solução definitiva	Prazo de atendimento	Prazo de solução definitiva
06 (seis) horas	48 (quarenta e oito) horas	10 (dez) horas	48 (quarenta e oito) horas

**2.2.5.5 -** Severidade BAIXA: Esse nível de severidade é aplicado para a instalação, configuração, manutenções preventivas, aplicações de firmwares e esclarecimento técnico relativo ao uso da solução. Não haverá abertura de chamados de suporte técnico com esta severidade em sábados, domingos e feriados.

Dias úteis		Sábados, domingos e feriados	
Prazo atendimento	Prazo de solução definitiva	Prazo atendimento	Prazo de solução definitiva
30 (trinta) horas	72 (setenta e duas) horas	-	-

**2.2.5.6-** Serão considerados para efeitos dos prazos exigidos:

**2.2.5.6.1.** Prazo de Atendimento: Tempo decorrido entre a solicitação efetuada pela Equipe Técnica do TRE-PR à Prestadora de Serviço e o efetivo início dos trabalhos de manutenção.

**2.2.5.6.2.** Prazo de Solução Definitiva: Tempo decorrido entre a solicitação efetuada pela Equipe Técnica do TRE-PR à Prestadora de Serviço e a efetiva recolocação dos equipamentos em seu pleno estado de funcionamento e operação normais.

**2.2.5.7 -** A contagem do prazo de atendimento e solução definitiva de cada solicitação será a partir da notificação ao licitante vencedor, até o momento da comunicação da solução definitiva do problema e aceite pela equipe técnica do TRE-PR;

**2.2.5.8 -** O atendimento às solicitações de severidade ALTA deverá ser realizado nas instalações da TRE-PR (on-site) e não poderá ser interrompido até o completo restabelecimento do serviço, mesmo que se estenda para períodos noturnos, sábados, domingos e feriados. Nesse caso, não poderá implicar em custos adicionais ao TRE-PR. A interrupção do suporte técnico de uma solicitação desse tipo de severidade por parte do licitante vencedor e que não tenha sido previamente autorizado pelo TRE-PR, poderá ensejar em aplicação de sanções previstas.

**2.2.5.9-** As ordens de serviços classificadas com severidade MÉDIA, quando não solucionados no prazo definido, poderão ser automaticamente escaladas para a severidade ALTA, sendo que os prazos de atendimento e solução definitiva do problema, bem como sanções previstas, serão automaticamente ajustados para o novo nível. A interrupção do suporte técnico de uma solicitação desse tipo de severidade por parte do licitante vencedor e que não tenha sido previamente autorizado pelo TRE-PR, poderá ensejar na aplicação das sanções previstas.

**2.2.5.10-** Depois de concluído o suporte técnico, o licitante vencedor comunicará o fato à Equipe Técnica do TRE-PR e solicitará autorização para o fechamento do chamado. Caso o TRE-PR não confirme a solução definitiva do problema, o chamado permanecerá aberto até que seja efetivamente solucionado pelo licitante vencedor. Nesse caso, o TRE-PR fornecerá as pendências relativas à solicitação em aberto.

**2.2.5.11-** O TRE-PR encaminhará a contratada, quando da reunião de apresentação inicial, relação nominal da equipe técnica autorizada a abrir e fechar solicitações de suporte técnico.

**2.2.5.12** - Por necessidade excepcional de serviço, o TRE-PR também poderá solicitar a escalação de chamado para níveis superiores de severidade. Nesse caso, a escalação deverá ser justificada e os prazos dos chamados passarão a contar do início novamente.

### **3 - DAS OBRIGAÇÕES DA CONTRATADA**

#### **3.1 – Da entrega:**

##### **3.1.1 – Do prazos:**

**3.1.1.1 – Prazo de entrega da solução:** a solução deverá ser entregue em um prazo de até **60 (sessenta) dias corridos**, a contar da assinatura do contrato.

**3.1.1.2 – Prazo de instalação e configuração:** a solução deverá ser instalada e configurada em um prazo de até **60 (sessenta) dias corridos**, contados da data de recebimento provisório.

**3.1.2 – Do local de entrega:** a solução deverá ser entregue no Tribunal Regional Eleitoral do Paraná, Rua João Parolin, nº 224, Curitiba-PR, Seção de Rede, agendamento pelos telefones (41) 3330-8628 ou 3330-8629.

#### **3.2 - – Do recebimento do objeto:**

**3.2.1 – Do recebimento provisório:** em até 10 (dez) dias corridos a solução será recebida, provisoriamente, para efeito de posterior verificação de sua conformidade com as especificações constantes neste Termo de Referência.

**3.2.2 – O recebimento provisório** será realizado pela Seção de Gestão de Equipamentos de Microinformática.

**3.2.3 -** Na hipótese de constatação de anomalias que comprometam a utilização adequada da solução, ela será rejeitada, em todo ou em parte, conforme dispõe o Art. 76 da Lei nº 8.666/93, sem qualquer ônus para o TRE-PR, devendo o licitante vencedor reapresentá-la (s) no prazo máximo de até 30 (trinta) dias, após o comunicado.

**3.2.4 – Do recebimento definitivo:** a verificação da conformidade das especificações da solução ocorrerá no prazo de até 10 (vinte) dias corridos, contados a partir do recebimento provisório. Atestada a conformidade quantitativa e qualitativa, a solução será recebida definitivamente.

**3.2.4.1-** O recebimento definitivo será realizado pela Coordenadoria de Infraestrutura.

#### **3.3 – Da garantia:**

**3.3.1 -** A solução ofertada deverá estar coberta por garantia total fornecida pelo fabricante, pelo prazo de 36 (trinta e seis) meses.

**3.3.1.1 -** A garantia iniciará a partir da data de recebimento definitivo da solução.

**3.3.2** - A contratada deverá apresentar o Certificado de Garantia emitido pelo fabricante, no prazo de até 30 (trinta) dias corridos, a contar da data de recebimento definitivo da solução.

**3.3.3** - A contratada deverá possibilitar a abertura de chamado técnico diretamente no fabricante da solução ou por centro de suporte devidamente autorizado pelo fabricante.

**3.3.4** - O atendimento de primeiro nível deve ser realizado em português do Brasil.

**3.3.5** - Deve ser disponibilizado pelo menos um dos seguintes canais de atendimento para suporte:

- a) Telefone 0800;
- b) Sistema Web de abertura de chamados;
- c) E-mail.

**3.3.6** - A Contratada deverá disponibilizar o acesso direto à base de dados de conhecimento do fabricante da solução que contenha informações de assistência, orientação para instalação, desinstalação, configuração, atualização de *firmware e software*, aplicação de correções (patches), diagnóstico, avaliações e resolução de problemas, e demais atividades relacionadas à correta operação, e funcionamento da solução.

**3.3.7** - A Contratada deverá, semestralmente, revisar as atualizações de drivers, firmwares e microcódigos de todos os *appliances* contratados. Os serviços de atualizações de *firmwares* somente deverão ocorrer para os eventos classificados como críticos.

**3.3.8** - Os serviços cobertos pela garantia deverão ser prestados nas instalações do TRE-PR, em Curitiba/PR.

**3.3.9** - Os serviços cobertos pela garantia deverão ser prestados pela empresa fabricante, pela contratada ou parceiro autorizado/credenciado, através da disponibilização de técnicos certificados pelo fabricante da solução.

**3.3.10** - A Contratada deverá fornecer a seus técnicos as ferramentas e instrumentos necessários à execução dos serviços, bem como produtos ou materiais indispensáveis à manutenção do equipamento.

**3.3.11** - Os discos rígidos que forem substituídos ou no caso de troca de equipamento ficarão retidos e serão de propriedade do TRE-PR.

**3.3.12** - A Contratada deverá garantir atualizações do produto e suporte técnico do fabricante (telefone, e-mail ou acesso remoto) pelo período de vigência da garantia.

**3.3.13** - A substituição de equipamento defeituoso deverá ocorrer em até 30 (trinta) dias corridos, após a abertura de Ordem de Serviço pelo gestor de contrato ou notificação automática do sistema na central de atendimento do licitante vencedor ou fabricante.

**3.4** - A Contratada deverá apresentar, ao gestor da contratação, em até 30 (trinta) dias corridos contados da assinatura do contrato, no momento da entrega dos equipamentos, os documentos abaixo:

a) Certificação/declaração emitida pelo fabricante do equipamento ofertado (ou credenciado) para, no mínimo, 02 (dois) funcionários, atestando participação em curso/treinamento específico relacionado à utilização/configuração/suporte do equipamento ofertado.

b) Comprovação do vínculo dos funcionários certificados (conforme alínea a) com a empresa contratada, mediante apresentação de carteira profissional ou contrato de prestação de serviços.

### **3.5 – Da sustentabilidade:**

**3.5.1** - Será exigida a compatibilidade do produto com a diretiva RoHS (RoHS - Restriction of Certain Hazardous Substances ou Restrição de Certas Substâncias Perigosas), a qual limita a um percentual máximo o uso de substâncias perigosas nos processos de fabricação dos produtos, entre elas: cádmio (Cd), mercúrio (Hg), cromo hexavalente (CrVI), bifenilos polibromados (PBBs), éteres difenil-polibromados (PBDEs) e chumbo (Pb), de modo a contribuir para a redução do impacto ambiental.

**3.5.2** - Os produtos deverão ser preferencialmente, acondicionados em embalagem individual adequada, com menor volume possível, que utilize materiais recicláveis, de forma a garantir a máxima proteção durante o transporte e o armazenamento. As condições deste item serão objeto de verificação *in loco* no momento da entrega dos produtos.

**3.6** - A contratada obrigar-se-á em manter-se em compatibilidade com a habilitação e com as obrigações assumidas na licitação até o adimplemento total da contratação.

## **4 - DISPOSIÇÕES GERAIS**

**4.1** - As licitantes deverão efetuar suas cotações seguindo rigorosamente as especificações solicitadas, abstendo-se de participar da licitação aqueles que não puderem atender às condições do edital.

**4.2** - Dúvidas referentes à contratação poderão ser sanadas com o servidor Breno Schult, pelo telefone: (41) 3330-8621 ou 3339-8681, das 12h às 19:00.





## Anexo II – Proposta Detalhada

A licitante classificada em primeiro lugar deverá encaminhar, em até 02 (duas) horas, a partir da solicitação do Pregoeiro, esta proposta detalhada, devidamente adequada ao lance final (conforme item 8.3 do edital), ficando ciente de que caso não seja encaminhada, ensejará a desclassificação, sendo convocada a licitante classificada em 2º lugar para atender ao disposto acima e assim sucessivamente.

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.

Empresa: Data:			
ITEM	DISCRIMINAÇÃO	QUANT.	Valor Unitário
	(equipamento e modelo)		
	(acessórios)		
	(licenciamento)		
	(sítio da internet para consulta da documentação)		

### ANEXO III

#### “MINUTA”

#### TRIBUNAL REGIONAL ELEITORAL DO PARANÁ ATA DE REGISTRO DE PREÇOS

O Tribunal Regional Eleitoral do Paraná, situado na Rua João Parolin nº 224 - Parolin, 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 10.024/2019, nº 7.892/13 e demais normas legais aplicáveis, em face da classificação da proposta apresentada no Pregão Eletrônico nº xx/201x (PAD 6279/2019), 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	PREÇO UNITÁRIO (R\$)

## 1. DO OBJETO

**1.1** - A presente Ata tem por objeto o Registro de Preços para solução de proteção de rede com características de *Next Generation Firewall (NGFW)* para segurança de informação perimetral que inclui filtro de pacotes, controle de aplicação, administração de largura de banda (QoS), VPN IPSec e SSL, IPS, prevenção contra ameaças de vírus, *spywares e malwares "Zero Day"*, Filtro de URL, funcionalidade de *Sandbox*, bem como controle de transmissão de dados e acesso à Internet compondo uma plataforma de segurança integrada, 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 e-mail 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 prestação de serviço, desde que observadas as normas de segurança;
- c) notificar o fornecedor de qualquer irregularidade encontrada na prestação do serviço;
- 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 contratação 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) prestar os serviços solicitados nos prazos máximos estabelecidos no item 3.1.1 do 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.

**3.2** – Não será permitida a adesão à esta Ata de Registro de Preços por órgãos ou entidades que não participaram do certame licitatório.

### **4. DO GERENCIAMENTO DA ATA DE REGISTRO DE PREÇOS**

**4.1** - O gerenciamento da Ata de Registro de Preços será feito por servidor formalmente designado, que determinará 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 à prestação do serviço efetuada 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 na prestação dos serviços ora contratada, 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 através 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 prestação 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 prestar os serviços 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) obrigam-se a 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 IV).**

## **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 da 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 aceite 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 2019.

\_\_\_\_\_  
(Assinatura Representante legal)

CARGO: .....

\_\_\_\_\_  
Dr. Valcir Mombach  
Diretor-Geral do TRE/PR



CONTRATO Nº ...../201...

PAD nº 006279/2019

#### ANEXO IV

#### MINUTA DO CONTRATO

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

Pelo presente instrumento, regido pela Lei nº 8.666 de 21.06.93, regida pela Lei nº 10.520/02, Lei Complementar nº 123/06, Lei nº 11.488/2007, pelos Decretos nº 10.024/2019 e nº 8.538/2015, e em conformidade com o Termo de Abertura de Licitação nº 38/2019, Pregão Eletrônico nº. ..../2019- Registro de Preços, e a proposta vencedora, protocolada neste Tribunal sob o nº. 6279/2019, regularmente autorizada pelo ordenador de despesas;

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, neste ato representado por sua Diretor-Geral, Dr. Valcir Mombach, doravante denominado CONTRATANTE, e a empresa:

....., inscrita no CNPJ sob nº  
....., com sede em Cidade/UF, na Rua ....., nº. ...., bairro  
....., CEP: ....., telefone: (...) ....., e-mail: .....,  
neste ato representada por ....., portador do CPF/MF nº.  
....., doravante denominada CONTRATADA; têm entre si justo e  
acertado o que segue:

#### CLÁUSULA PRIMEIRA: DO OBJETO

**1.1** – A presente contratação tem por objeto o **fornecimento e garantia** de solução de proteção de rede com características de **Next Generation Firewall (NGFW)** para segurança de informação perimetral que inclui filtro de pacotes, controle de aplicação, administração de largura de banda (QoS), VPN IPsec e SSL, IPS, prevenção contra

ameaças de vírus, *spywares* e *malwares* “Zero Day”, Filtro de URL, funcionalidade de *Sandbox*, bem como controle de transmissão de dados e acesso à Internet compondo uma plataforma de segurança<sup>1</sup> integrada com garantia e respectiva subscrição por, pelo menos, 36 (trinta e seis) meses, serviços de instalação e treinamento, conforme especificações descritas neste Contrato.

**1.2** - A Contratação obedecerá ao estipulado neste contrato, bem como às disposições do instrumento convocatório, que, independentemente de transcrição, fazem parte integrante e complementar deste.

## CLÁUSULA SEGUNDA: DAS ESPECIFICAÇÕES TÉCNICAS

**2.1** – Aquisição dos itens abaixo informados: (*adequar o item e quantidade conforme o pedido do item respectivo*)

	Item	Descrição	Quantidade
LOTE 1	1	<i>Appliance Next Generation Firewall (NGFW)</i> , com interface de gerência e respectivas licenças, garantia, suporte e atualizações por 36 meses	....
	2	Licenças, garantia, suporte e atualizações por período adicional de 24 meses para toda a solução apresentada no item 1	.....
	3	Serviços de instalação, configuração e repasse de conhecimento	.....
	4	Treinamento	.....

**2.2** - Descrição dos itens e requisitos técnicos mínimos:

(*adequar conforme item solicitado do lote acima*)

### **2.2.1 – ITEM 1 - *Appliance Firewall NGFW*:**

**2.2.1.1** - Entende-se por “*Appliance Firewall NGFW*”, conjunto formado por *hardware* e respectivas licenças de *software* necessárias para seu funcionamento, incluídas as consoles de gerência e monitoramento.

**2.2.1.1.1** - Para atendimento a esse item será aceito o fornecimento do *hardware* em *appliance* composto por 02 (dois) equipamentos, desde que atendidas todas as características, as funcionalidades e as capacidades descritas neste termo de referência.

**2.2.1.2** - Cada “*Appliance NGFW*” deve possuir as seguintes características, licenciadas para uso:

**2.2.1.2.1** - Possuir *throughput* mínimo de 2 Gbps 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, Antivírus e *Anti-spyware*. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será considerado.

<sup>1</sup> Por plataforma de segurança entende-se hardware e software integrados do tipo *appliance*

**2.2.1.2.2** - Os *throughputs* devem ser comprovados por documento de domínio público do fabricante. A localização destes documentos deve ser informada na proposta detalhada (conforme item 8.3 do edital). A ausência/inexistência de tais documentos resultará desclassificação da proposta.

**2.2.1.2.3** - Os documentos públicos devem comprovar os *throughputs* aferidos com tráfego HTTP ou **blend** de protocolos definidos pelo fabricante como tráfego real (*real-world traffic blend*).

**2.2.1.2.4** - Não será aceita aceleração de pacotes na placa de rede limitando a análise somente até camada 4.

**2.2.1.2.5** - Deve ser capaz de suportar, no mínimo, 1.000.000 conexões simultâneas.

**2.2.1.2.6** - Deve ser capaz de suportar, no mínimo, 55.000 novas conexões por segundo.

**2.2.1.2.7** - Deve ser fornecido com fontes 120/240 AC, redundantes, ou seja, estes elementos devem permitir a sua substituição sem que seja necessário desligar o equipamento.

**2.2.1.2.8** - Deve ser fornecido com *coolers* ou *fans hot-swappable*s, ou seja, estes elementos devem permitir a sua substituição sem que seja necessário desligar o equipamento.

**2.2.1.2.9** - Deve ser fornecido com disco *Solid State Drive* (SSD) com no mínimo 2400 GB.

**2.2.1.2.10** - Deve possuir, no mínimo, 08 (oito) interfaces de rede 10/100/1000 base-TX.

**2.2.1.2.11** - Deve possuir, no mínimo, 04 (quatro) interfaces de rede 10 Gbps SFP+, fornecidos com seus respectivos *transceivers* do tipo SR.

**2.2.1.2.12** - Deve possuir 01 (uma) interface de rede 1 Gbps dedicada para gerenciamento.

**2.2.1.2.13** - Deve possuir 01 (uma) interface do tipo console ou similar.

**2.2.1.2.14** - Deve ser capaz de operar em alta disponibilidade nos modos Ativo/Ativo ou Ativo/Passivo.

**2.2.1.2.15** - Os equipamentos (*appliances*) fornecidos (Alta disponibilidade) devem possuir o mesmo fabricante, modelo e configuração.

**2.2.1.2.16** - Deve suportar, no mínimo, 50 (cinquenta) zonas de segurança.

**2.2.1.2.17** - Deve permitir a expansão futura de, no mínimo, 04 (quatro) instâncias virtuais de *firewall*.

**2.2.1.2.18** - Deve ser fornecido com licenciamento ou suporte sem a necessidade de licença adicional para, no mínimo, 300 (trezentos) clientes de VPN SSL simultâneos.

**2.2.1.2.19** - Deve ser fornecido com licenciamento ou suporte sem a necessidade de licença adicional para, no mínimo, 50 (cinquenta) túneis de VPN IPSEC simultâneos.



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

**2.2.1.4 -** Por console de gerência e monitoração, entende-se as licenças de *software* necessárias para as duas funcionalidades.

**2.2.1.5 -** A console de gerência e monitoramento não pode residir no mesmo *appliance* de proteção de rede, devendo ser segregadas dos equipamentos dos *appliances* de proteção.

**2.2.1.5.1 -** A console de gerência e monitoramento deve ser virtual e deve rodar em ambiente VMWare ESXi 6.0 ou superior.

**2.2.1.6 -** Na data da proposta, nenhum dos modelos ofertados poderá estar listado no site do fabricante em como *end-of-life* ou *end-of-sale*.

**2.2.1.7 -** Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19", e devem incluir kit tipo trilho para adaptação, se necessário, e cabos de alimentação.

**2.3.1.8 -** A solução deve consistir de *appliance* de proteção de rede com funcionalidades de *Next Generation Firewall* (NGFW), e console de gerência e monitoração.

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

**2.2.1.10 -** As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos *appliances* desde que obedeçam a todos os requisitos desta especificação.

**2.2.1.11 -** A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7.

**2.2.1.12 -** O *hardware* e *software* que executem as funcionalidades de proteção de rede, bem como a console de gerência e monitoração, devem ser do tipo *appliance*. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico.

**2.2.1.13 -** O *software* deverá ser fornecido em sua versão mais atualizada recomendada pelo fabricante.

**2.2.1.14 -** Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:

- a) Suporte a 1024 VLAN Tags 802.1q
- b) Agregação de links 802.3ad e LACP
- c) Policy based routing ou policy based forwarding
- d) Roteamento multicast (PIM-SM)
- e) DHCP Relay
- f) DHCP Server
- g) Suporte à criação de objetos de rede

**2.2.1.15 -** Suportar sub-interfaces ethernet logicas.

**2.2.1.15.1 -** Suporte a, no mínimo, 10 (dez) roteadores virtuais na mesma instância de *firewall* ou roteamento baseado em políticas (PBR).

**2.2.1.16 -** O *firewall* deve ter a capacidade de testar o funcionamento de rotas estáticas ou rota *default* com a definição de um endereço IP de destino que deve estar comunicável por meio de uma rota. Caso haja falha na comunicação o *firewall* deve ter a capacidade de usar rota alternativa para estabelecer a comunicação.

**2.2.1.17 -** Deve suportar os seguintes tipos de NAT:

- a) Nat dinâmico (*Many-to-1*);
- b) Nat dinâmico (*Many-to-Many*);
- c) Nat estático (1-to-1);
- d) NAT estático (*Many-to-Many*);
- e) Nat estático bidirecional 1-to-1;
- f) Tradução de porta (PAT);
- g) NAT de Origem;
- h) NAT de Destino;
- i) Suportar NAT de Origem e NAT de Destino simultaneamente.

**2.2.1.18 -** Deve implementar o protocolo ECMP.

**2.2.1.19 -** Deve implementar balanceamento de link por pelo menos um dos métodos a seguir: IP de origem, IP de origem e destino ou *round-robin*.

**2.2.1.20 -** Enviar log para sistemas de monitoração externos, simultaneamente.

**2.2.1.21 -** Deve haver a opção de enviar logs para os sistemas de monitoração externos.

**2.2.1.22 -** Proteção de *anti-spoofing*;

**2.2.1.23 -** Dever permitir bloquear conexões que contenham dados no *payload* de pacotes durante o *three-way hand-shake*;

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

**2.2.1.25 -** Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2).

**2.2.1.26 -** Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3).

**2.2.1.27 -** Suportar a OSPF *graceful restart*;

**2.2.1.28 -** Deve suportar o protocolo BGP permitindo que o *firewall* possa anunciar rotas para IPv6.

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

**2.2.1.29 -** Os dispositivos de proteção devem ter a capacidade de operar mediante o uso de suas interfaces físicas nos seguintes modos: Modo *sniffer* (monitoramento e análise do tráfego de rede), camada 2 (I2) e camada 3 (I3).

**2.2.1.29.1 -** Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede.

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

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

**2.2.1.30** - Suporte à configuração de alta disponibilidade Ativo/Passivo ou Ativo/Ativo:

- a) Em modo transparente;
- b) Em layer 3.

**2.2.1.31** - A configuração em alta disponibilidade deve sincronizar:

- a) Sessões;
- b) Configurações, incluindo, mas não limitado a políticas de *Firewall*, NAT, QOS e objetos de rede;
- c) Associações de Segurança das VPNs;
- d) Tabelas FIB.

**2.2.1.32** - O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link.

**2.2.1.33** - As funcionalidades de filtro de pacotes, NAT, VPN IPsec e protocolos de roteamento dinâmico devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de *software* com o fabricante.

**2.2.1.34 - Controle por política de *Firewall***

**2.2.1.34.1** - Deverá suportar controles por zona de segurança.

**2.2.1.34.2** - Controles de políticas por porta e protocolo.

**2.2.1.34.3** - Cada regra deve, obrigatoriamente, funcionar nas versões de endereço IP 4 e 6 sem duplicação da base de objetos e regras.

**2.2.1.34.4** - A solução deve identificar de forma automática quais interfaces o tráfego irá ser direcionado, evitando assim que as interfaces de origem e destino tenham que ser obrigatoriamente explicitadas ou obrigatoriamente listadas.

**2.2.1.34.5** - Controle de políticas por aplicações grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações.

**2.2.1.34.6** - Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;

**2.2.1.34.7** - Deve permitir consultar ou criar políticas para objetos das listas externas ou nuvem de inteligência do fabricante a partir da interface de gerência do próprio firewall.

**2.2.1.34.8** - Controle de políticas por código de País (Por exemplo: BR, USA, UK, RUS).

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

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

**2.2.1.34.11** - Deve de-criptografar sites e aplicações que utilizam certificados ECC, incluindo *Elliptical Curve Digital Signature Algorithm (ECDSA)*;

**2.2.1.34.12** - Controle de inspeção e de-criptografia de SSH ou SSL por política.

**2.2.1.34.13** - Bloqueio de, no mínimo, os seguintes tipos de arquivos: cab, msi e exe.

**2.2.1.34.14** - *Traffic shaping* QoS baseado em Políticas (Prioridade, Garantia e Máximo).

**2.2.1.34.15** - Suporte a objetos e regras IPV6.

**2.2.1.34.16** - Suporte a objetos e regras *multicast*.

**2.2.1.34.17** - Deve suportar no mínimo dois dos tipos de negação de tráfego nas políticas de *firewall* a seguir: Drop sem notificação do bloqueio ao usuário, Drop com opção de envio de ICMP *Unreachable* para máquina de origem do tráfego, TCP-Reset para o client, TCP-Reset para o server ou para os dois lados da conexão.

**2.2.1.34.18** - Suportar a atribuição de agendamento das políticas (ou regras) com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.

#### **2.2.1.35 - Controle de aplicações**

**2.2.1.35.1** - Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo.

**2.2.1.35.2** - Deve ser possível efetuar a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos.

**2.2.1.35.3** - Deve reconhecer nativamente aplicações relacionadas a tráfego *peer-to-peer*, redes sociais, acesso remoto, *update* de *software*, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail.

**2.2.1.35.4** - Deve reconhecer pelo menos as seguintes aplicações: *bittorrent*, *gnutella*, *skype*, *facebook*, *linked-in*, *twitter*, *citrix*, *logmein*, *teamviewer*, *rdp* ou *ms-rdp*, *vnc*, *gmail*, *youtube*, *http-tunnel*, *facebook chat*, *gmail chat*, *whatsapp*, *4shared*, *dropbox*, *google drive*, *onedrive*, *db2*, *mysql*, *oracle*, *kerberos*, *ldap*, *radius*, *itunes*, *dhcp*, *ftp*, *dns*, *wins*, *ntp*, *snmp*, *gotomeeting*, *webex*, *evernote* e *google* ou *google-docs*;

**2.2.1.35** - Deve inspecionar o *payload* de pacote de dados com o objetivo de detectar por meio de expressões regulares assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo. A checagem de assinaturas também deve determinar se uma aplicação está utilizando a porta *default* ou não, incluindo, mas não limitado a RDP na porta 80 ao invés de 3389;

**2.2.1.35.6** - Deve detectar aplicações por meio de análise comportamental do tráfego observado, incluindo, pelo menos, *Encrypted Bittorrent* e aplicações VOIP.

**2.2.1.35.7** - 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 ataques mediante a porta 443.

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

**2.2.1.35.9** - Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado a *Yahoo Instant Messenger* usando HTTP. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do *Webex*. Além de detectar arquivos e outros conteúdos que devem ser inspecionados de acordo as regras de segurança implementadas.

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

**2.2.1.35.11** - Deve permitir controle granular para aplicações SaaS, tais como: *Office 365*, *Skype*, aplicativos *google*, *gmail*, etc.;

**2.2.1.35.12** - Identificar o uso de táticas evasivas via comunicações criptografadas;

**2.2.1.35.13** - Atualizar a base de assinaturas de aplicações automaticamente.

**2.2.1.35.14** - Reconhecer aplicações em IPv6.

**2.2.1.35.15** - Limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD.

**2.2.1.35.16** - Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente nas estações dos usuários.

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

**2.2.1.35.18** - Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos: checagem de assinaturas e decodificação de protocolos.

**2.2.1.35.19** - Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas.

**2.2.1.35.20** - Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações da instituição.

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



**2.2.1.35.21** - O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações.

**2.2.1.35.22** - Deve alertar o usuário quando uma aplicação for bloqueada.

**2.2.1.35.23** - Deve possibilitar que o controle de portas seja aplicado para todas as aplicações.

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

**2.2.1.35.25** - Deve possibilitar a diferenciação de tráfegos de *Instant Messaging* (*AIM*, *Gtalk*, *Facebook Chat*, etc.) possuindo granularidade de controle/políticas para os mesmos.

**2.2.1.35.26** - Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o *Gtalk* chat e bloquear a transferência de arquivos.

**2.2.1.35.27** - Deve possibilitar a diferenciação de aplicações *Proxies* (*ghostsurf*, *free-gate*, etc.) possuindo granularidade de controle/políticas para os mesmos.

**2.2.1.35.28** - Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como:

- a) Tecnologia utilizada nas aplicações (*Client-Server*, *Browser Based*, *Network Protocol*, etc.);
- b) Nível de risco da aplicação;
- c) Categoria e subcategoria de aplicações;
- d) Aplicações que usem técnicas evasivas, utilizadas por *malwares*, como transferência de arquivos e/ou uso excessivo de banda, etc.

#### **2.2.1.36 - Prevenção de ameaças**

**2.2.1.36.1** - Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e *Anti-Spyware* (ou *antimalware*) integrados no próprio *appliance* de *Firewall* ou entregue por meio de composição com outro equipamento ou fabricante.

**2.2.1.36.2** - Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e *Anti-Spyware* ou *antimalware*).

**2.2.1.36.3** - Deve sincronizar as assinaturas de IPS, Antivírus, *Anti-Spyware* (ou *antimalware*) quando implementado em alta disponibilidade ativo/ativo ou ativo/passivo.

**2.2.1.36.4** - Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS e *Anti-spyware* ou *antimalware*: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo e enviar *reset* ou *tcp-reset*.

**2.2.1.36.5** - Deve possuir a capacidade de detectar e prevenir contra ameaças em tráfegos HTTP/2.

**2.2.1.36.6** - As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração.

**2.2.1.36.7** - Exceções por IP de origem ou de destino devem ser possíveis nas regras, de forma geral e assinatura a assinatura;

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

**2.2.1.36.9** - Deve permitir o bloqueio de vulnerabilidades.

**2.2.1.36.10** - Deve permitir o bloqueio de *exploits* conhecidos.

**2.2.1.36.11** - Deve incluir proteção contra ataques de negação de serviços.

**2.2.1.36.12** - Deverá possuir os seguintes mecanismos de inspeção de IPS:

- a) Análise de padrões de estado de conexões;
- b) Análise de decodificação de protocolo;
- c) Análise para detecção de anomalias de protocolo;
- d) IP Defragmentation;
- e) Remontagem de pacotes de TCP;
- f) Bloqueio de pacotes malformados.

**2.2.1.36.13** - Ser imune e capaz de impedir ataques básicos como: Synflood, ICMPflood e UDPflood.

**2.2.1.36.14** - Detectar e bloquear a origem de *portscans* com possibilidade de criar exceções para endereços IPs de ferramentas de monitoramento da instituição.

**2.2.1.36.15** - Bloquear ataques efetuados por *worms* conhecidos, permitindo ao administrador acrescentar novos padrões.

**2.2.1.36.16** - Possuir tecnologia ou assinaturas para a mitigação de ataques DoS e DDoS.

**2.2.1.36.17** - Possuir assinaturas para bloqueio de ataques de buffer overflow.

**2.2.1.36.18** - Deverá possibilitar a criação de assinaturas customizadas pelo órgão.

**2.2.1.36.19** - Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS, permitindo a criação de exceções com granularidade nas configurações.

**2.2.1.36.20** - Permitir o bloqueio de vírus e *spywares* (ou *malwares*) em, pelo menos, os seguintes protocolos: HTTP, HTTPS, SMB ou NetBios-ssn e SMTP;

**2.2.1.36.20.1** - É permitido uso de *appliance* externo (antivírus de rede), para o bloqueio de vírus e **spywares** em protocolo SMB de forma a conter *malwares* se espalhando horizontalmente pela rede.

**2.2.1.36.21** - Suportar bloqueio de arquivos por tipo.

**2.2.1.36.22** - Deve estar apto a identificar e bloquear comunicação com botnets.

**2.2.1.36.23** - Deve suportar várias técnicas de prevenção, incluindo Drop e tcp-rst.

**2.2.1.36.24** - Registrar na console de monitoração as seguintes informações sobre ameaças identificadas.

**2.2.1.36.24.1** - O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

**2.2.1.36.25** - Deve suportar a captura de pacotes (PCAP), por assinatura de IPS e *Anti-spyware*.

**2.2.1.36.26** - Deve possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos sejam resolvidas pelo Firewall com endereços (IPv4 ou IPv6), previamente definidos.

**2.2.1.36.27** - Os eventos devem identificar o país de onde partiu a ameaça.

**2.2.1.36.28** - Proteção contra downloads involuntários usando HTTP de arquivos executáveis maliciosos.

**2.2.1.36.29** - Rastreamento de vírus em pdf.

**2.2.1.36.30** - Deve permitir a inspeção em arquivos comprimidos que utilizam o algoritmo *deflate* (zip, gzip, etc.).

**2.2.1.36.31** - 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.

### **2.3.1.37 - Análise de *malwares***

**2.2.1.37.1** - Devido aos *Malwares* hoje em dia serem muito dinâmicos e um antivírus comum reativo não ser capaz de detectar os mesmos com a mesma velocidade que suas variações são criadas, a solução ofertada deve possuir funcionalidades para análise de *Malwares* não conhecidos incluídas na própria ferramenta ou entregue com composição com outro fabricante.

**2.2.1.37.2** - O dispositivo de proteção deve ser capaz de enviar arquivos trafegados de forma automática para análise "*In Cloud*" ou local, onde o arquivo será executado e simulado em ambiente controlado.

**2.2.1.37.3** - A solução deve ser capaz de selecionar por meio de políticas granulares quais tipos de arquivos sofrerão esta análise incluindo, mas não limitado a: endereço IP de origem/destino, usuário/grupo do AD/LDAP, aplicação, porta, URL/categoria de URL de destino, tipo de arquivo e todas estas opções simultaneamente;

**2.2.1.37.4** - Deve possuir a capacidade de diferenciar arquivos analisados em pelo menos duas das três categorias: malicioso, não malicioso e arquivos não maliciosos, mas com características indesejáveis (como softwares que deixa o sistema operacional lento, que alteram parâmetros do sistema, etc.).

**2.2.1.37.5** - Suportar a análise com pelo menos 50 (cinquenta) tipos de comportamentos maliciosos para a análise da ameaça não conhecida.

**2.2.1.37.6** - Suportar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional *Windows 7* e *Windows 10*;

**2.2.1.37.7** - Deve suportar a monitoração de arquivos trafegados na internet (HTTPs, HTTP e SMTP).

**2.2.1.37.8** - A solução deve possuir a capacidade de analisar em *sandbox links* (http e HTTPS) presentes no corpo de e-mails trafegados em SMTP. Deve ser gerado um relatório caso a abertura do link pela *sandbox* o identifique como site hospedeiro de *exploits*.

**2.2.1.37.9** - Para ameaças trafegadas em protocolo SMTP, a solução deve ter a capacidade de mostrar nos relatórios o remetente, destinatário e assunto dos *e-mails* permitindo identificação ágil do usuário vítima do ataque.

**2.2.1.37.10** - O sistema de análise *"In Cloud"* ou local deve prover informações sobre as ações do *Malware* na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo *Malware*, gerar assinaturas de Antivírus e *Anti-spyware* automaticamente, definir URLs não confiáveis utilizadas pelo novo *Malware* e prover informações sobre o usuário infectado (seu endereço IP e seu login de rede).

**2.2.1.37.11** - Deve permitir o download dos *malwares* identificados a partir da própria interface de gerência.

**2.2.1.37.12** - Deve permitir informar ao fabricante quanto a suspeita de ocorrências de falso-positivo e falso-negativo na análise de *malwares* de dia zero.

**2.2.1.37.13** - Caso a solução de análise de *malware* seja fornecida em *appliance* local, deve possuir, no mínimo, 25 ambientes controlados (*sandbox*) independentes para execução simultânea de arquivos suspeitos.

**2.2.1.37.14** - Caso sejam necessárias licenças de sistemas operacional e softwares para execução de arquivos no ambiente controlado (*sandbox*), as mesmas devem ser fornecidas em sua totalidade, sem custos adicionais para a contratante.

**2.2.1.37.15** - Suportar a análise de arquivos executáveis, ZIP e criptografados em SSL no ambiente controlado.

**2.2.1.37.16** - Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos Java (.jar), Linux (ELF), RAR e 7-ZIP no ambiente de *sandbox*;

**2.2.1.37.17** - Permitir o envio de arquivos e links para análise no ambiente controlado de forma automática via API.

### **2.3.1.38- Filtro de URL**

**2.2.1.38.1** - A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL.

**2.2.1.38.1.1** - Permite especificar políticas por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

**2.2.1.38.1.2** - Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs, Redes e Zonas de segurança.

**2.2.1.38.1.3** - Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs por meio da integração com serviços de diretório, autenticação via ldap, Active Directory, E-directory e base de dados local.

**2.2.1.38.1.4** - Permitir popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório.

**2.2.1.38.1.5** - Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL.

**2.2.1.38.1.6** - Suportar base ou cache de URLs local no *appliance*, evitando **delay** de comunicação/validação das URLs.

**2.2.1.38.1.7** - Possui pelo menos 50 categorias de URLs.

**2.2.1.38.1.8** - Deve classificar o nível de risco de URLs ou aplicações em, pelo menos, três níveis: baixo, médio e alto.

**2.2.1.38.1.9** - A categorização de URL deve analisar toda a URL e não somente até o nível de diretório.

**2.2.1.38.1.10** - Permitir a criação categorias de URLs customizadas.

**2.2.1.38.1.11** - Permitir a exclusão de URLs do bloqueio, por categoria.

**2.2.1.38.1.12** - Permite a customização de página de bloqueio.

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

**2.2.1.38.1.14** - Suportar a inclusão nos logs do produto de informações das atividades dos usuários.

#### **2.2.1.39- Identificação de usuários**

**2.2.1.39.1** - Deve ser capaz de criar políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via ldap, *Active Directory* e base de dados local.

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

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

**2.2.1.39.4** - Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;

**2.2.1.39.4.1** - Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x ou soluções NAC via syslog ou radius, para a identificação de endereços IP e usuários.

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

**2.2.1.39.6** - Suportar a autenticação *Kerberos*.



**2.2.1.39.7** - Deve suportar autenticação via *Kerberos* para administradores da plataforma de segurança, *Captive Portal* e usuário de VPN SSL;

**2.2.1.39.8** - 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.

**2.2.1.39.9**- Deve implementar a criação de grupos customizados de usuários no *fire-wall*, baseado em atributos do LDAP/AD;

**2.2.1.39.10** -Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em servidores acessados remotamente.

#### **2.2.1.40 - QoS**

**2.2.1.40.1** - Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como *youtube*, *ustream*, etc.) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo *streaming*.

**2.2.1.40.2** - Suportar a criação de políticas de QoS por:

- a) Endereço de origem;
- b) Endereço de destino;
- c) Por usuário e grupo do LDAP/AD;
- d) Por aplicações, incluindo, mas não limitado a *Skype*, *Bittorrent* e *Youtube*;
- e) Por porta.
- f) O QoS deve possibilitar a definição de limite de *Upload* e *Download* ou de classes por: banda garantida, banda máxima e fila de prioridade.

**2.2.1.40.3** - Suportar a limitação de upload e download ou a priorização *Real Time* de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype.

**2.2.1.40.4** - Disponibilizar estatísticas *Real Time* para classes de QoS.

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

#### **2.2.1.41 - Filtro de dados**

**2.2.1.41.1** - Permitir a criação de filtros para arquivos e dados pré-definidos.

**2.2.1.41.2** - Os arquivos devem ser identificados por extensão e assinaturas.

**2.2.1.41.3** - Permitir a identificação e opcionalmente prevenir a transferência de vários tipos de arquivos (*Office*, PDF, etc.) identificados sobre aplicações (P2P, *Instant Messaging* etc.).

**2.2.1.41.4** - Suportar identificação de arquivos compactados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos.

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

**2.2.1.41.6** - Permitir listar o número de aplicações suportadas para controle de dados.

**2.2.1.41.7** - Permitir listar o número de tipos de arquivos suportados para controle de dados.

#### **2.2.1.42 - Geo-localização**

**2.2.1.42.1** - Suportar a criação de políticas por Geo-localização, permitindo que o tráfego de determinado País/Países seja bloqueado.

**2.2.1.42.2** - Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos.

**2.2.1.42.3** - Deve possibilitar a criação de regiões geográficas, caso a solução ofertada não possua as regiões pré-cadastradas, e criar políticas utilizando as mesmas para criar políticas utilizando as mesmas.

#### **2.2.1.43 - VPN IPSEC/SSL**

**2.2.1.43.1** - Suportar VPN Site-to-Site e Cliente-To-Site.

**2.2.1.43.2** - Suportar IPSec VPN.

**2.2.1.43.3** - Suportar SSL VPN.

**2.2.1.43.4** - A VPN IPsec deve suportar:

- a) DES e 3DES;
- b) Autenticação MD5 e SHA-1;
- c) *Diffie-Hellman Group 1, Group 2, Group 5 e Group 14*;
- d) Algoritmo *Internet Key Exchange* (IKEv1 e v2);
- e) AES 128 e 256 (*Advanced Encryption Standard*);
- f) Autenticação via certificado IKE PKI.

**2.2.1.43.5** - A VPN SSL deve suportar:

**2.2.1.43.5.1** - O usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB.

**2.2.1.43.5.2** - As funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente.

**2.2.1.43.5.3** - Atribuição de endereço IP nos clientes remotos de VPN SSL.

**2.2.1.43.5.4** - Deve permitir a atribuição de IPs fixos nos usuários remotos de VPN SSL.

**2.2.1.43.5.5** - Deve permitir a criação de rotas de acesso e faixas de endereços IP atribuídas a clientes remotos de VPN de forma customizada por usuário.

**2.2.1.43.5.6** - 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*.

**2.2.1.43.5.7** - Atribuição de DNS nos clientes remotos de VPN;

**2.2.1.43.5.8** - Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, *Anti-spyware* (ou *antimalware*) e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL.

**2.2.1.43.5.9** - Suportar autenticação via AD/LDAP, certificado e base de usuários local.

**2.2.1.43.5.10** - Permitir o estabelecimento de túnel VPN *client-to-site* do cliente a plataforma de segurança, integrando-se com as ferramentas de *Windows-logon*.

**2.2.1.43.5.11** - Suportar leitura e verificação de CRL (*certificate revocation list*).

**2.2.1.43.5.12** - O agente de VPN a ser instalado nos equipamentos desktop e laptops, dever ser capaz de ser distribuído de maneira automática via Microsoft SMS, Active Directory ou ser descarregado diretamente desde o seu próprio portal, o qual residirá no centralizador de VPN.

**2.2.1.43.5.13** - O agente deverá comunicar-se com o portal para determinar as políticas de segurança do usuário,

**2.2.1.43.5.14** - Deve permitir que a conexão com a VPN SSL seja estabelecida das seguintes formas:

- a) Após autenticação do usuário na estação;
- b) Sob demanda do usuário.

**2.2.1.43.5.15** - Deve manter uma conexão segura com o portal durante a sessão.

**2.2.1.43.5.16** - O agente de VPN SSL *client-to-site* deve ser compatível com pelo menos: *Windows Vista, Windows 7, Windows 8, Windows 10, Mac OSx, Android e IOS*.

**2.2.1.43.5.17** - Deve possuir a capacidade de identificar se a origem da conexão de VPN é externa ou interna.

**2.2.1.43.5.18** - Deve possuir mecanismos de checagem de conformidade do dispositivo remoto.

**2.2.1.43.5.19** - Para atendimento as funcionalidades de VPN IPSEC/SSL, será permitido a composição com solução de concentrador VPN por meio de *appliance* físico ou virtual desde que a solução proposta seja do mesmo fabricante e não implique em custo ou licença adicional.

## **2.2.1.44 - Console de gerência e monitoramento**

**2.2.1.44.1** - Deve possuir solução de gerenciamento centralizado, possibilitando o gerenciamento de diversos *appliances*.

**2.2.1.44.2** - O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos *appliances* da plataforma de segurança.

**2.2.1.44.3** - Controle sobre todos os *appliances* da plataforma de segurança em uma única console, com administração de privilégios e funções, salvo o concentrador VPN.

**2.2.1.44.4** - O gerenciamento centralizado deverá ser entregue como *appliance* virtual e deve ser compatível com *VMware ESXi 6.0* ou superior.

**2.2.1.44.5** - Deve permitir controle global de políticas para todos os *appliances* que compõe a plataforma de segurança.

**2.2.1.44.6** - Deve suportar organizar os *appliances* administrados em grupos: os grupos podem ser geográficos, por funcionalidade (por exemplo, IPS), e distribuição.

**2.2.1.44.7** - Deve implementar sistema de hierarquia entre os firewalls gerenciados, onde seja possível aplicar configurações de forma granular em grupos de *firewalls*.

**2.2.1.44.8** - Deve implementar a criação de perfis de usuários com acesso a plataforma de gerenciamento com definição exata de quais informações e de quais *firewalls* e grupos de *firewalls* o usuário terá acesso referente a logs e relatórios.

**2.2.1.44.9** - Deve permitir a criação de objetos.

**2.2.1.44.10** - Deve consolidar logs e relatórios de todos os *appliances* dispositivos administrados.

**2.2.1.44.11** - Deve permitir que exportar backup de configuração automaticamente via agendamento.

**2.2.1.44.12** - Deve permitir que a configuração ou pacote de atualização de versão dos *firewalls* seja importada de forma automática, ou manual, na plataforma de gerenciamento centralizado e que possa ser usada em outros *firewalls* e grupos de *firewalls*.

**2.2.1.44.13** - Deve mostrar os status dos *firewalls* em alta disponibilidade a partir da plataforma de gerenciamento centralizado.

**2.3.1.44.14** - Deve centralizar a administração de regras e políticas do cluster, usando uma única interface de gerenciamento.

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

**2.2.1.44.16** - Deve permitir substituir o certificado de fábrica no acesso HTTPS a gerência do *firewall* como possibilidade de uso de certificado criado localmente na própria solução ou importado de fonte externa.

**2.2.1.44.17** - Caso haja a necessidade de instalação de cliente para administração da solução o mesmo deve ser compatível com sistemas operacionais *Windows*.

**2.2.1.44.18** - O gerenciamento deve permitir/possuir:

- a) Criação e administração de políticas de *firewall* e controle de aplicação;
- b) Criação e administração de políticas de IPS, Antivírus e *Anti-Spyware* ou *Antimalware*;
- c) Criação e administração de políticas de Filtro de URL;
- d) Monitoramento de logs;
- e) Ferramentas de investigação de logs;
- f) Debugging;
- g) Captura de pacotes.

**2.2.1.44.19** - Acesso concorrente de administradores.

**2.2.1.44.20** - Deve permitir que administradores concorrentes façam modificações, validem e/ou revertam configurações do *firewall* simultaneamente e que cada administrador consiga aplicar apenas as suas alterações de forma independente das realizadas por outro administrador.

**2.2.1.44.21** - Deve mostrar ao administrador do *firewall* a hora e data do último login e tentativas de login com falha para acessos a partir da interface gráfica e CLI.

**2.2.1.44.22** - Deve possuir mecanismo busca global na solução onde possa se consultar, por uma *string*, elementos como: nome de objetos, ID ou nome de ameaças, nome de aplicações, nome de políticas e endereços IPs. Permitindo a localização e uso dos mesmos na configuração do dispositivo.

**2.2.1.44.23** - Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos.

**2.2.1.44.24** - Deve permitir monitorar via SNMP falhas de hardware e o uso de recursos do equipamento.

**2.2.1.44.25** - Bloqueio de alterações, no caso acesso simultâneo de dois ou mais administradores.

**2.2.1.44.26** - Permitir a definição de perfis de acesso à console com permissões granulares como: acesso de escrita e acesso de leitura.

**2.2.1.44.27** - Efetuar a autenticação integrada ao *Microsoft Active Directory* e servidor *Radius*.

**2.2.1.44.28** - Permitir efetuar buscas para localizar em quais regras um endereço IP, *IP Range*, *subnet* ou objetos estão sendo utilizados.

**2.2.1.44.29** - Deve atribuir sequencialmente um número a cada regra de *firewall*, NAT e QoS.

**2.2.1.44.30** - Permitir a criação de regras que fiquem ativas em horário definido.

**2.2.1.44.31** - Permitir a criação de regras com data de expiração.

**2.2.1.44.32** - Efetuar *backup* das configurações e *rollback* de configuração para a última configuração salva.

**2.2.1.44.33** - Permitir o *Rollback* de Sistema Operacional para a última versão local.

**2.3.1.44.34** - Permitir o upgrade via SCP ou interface de gerenciamento.

**2.2.1.44.35** - Permitir a validação regras antes da aplicação.

**2.2.1.44.36** - Deve implementar mecanismo de validação de configurações antes da aplicação das mesmas permitindo identificar erros.

**2.2.1.44.36.1** - Caso necessário, será aceito o uso de *appliance* externo para permitir a validação de regras antes da aplicação.

**2.2.1.44.37** - Deve possibilitar a visualização e comparação de configurações atuais, configuração anterior e configurações antigas.

**2.2.1.44.38** - Deve possibilitar a integração com a solução de SIEM em uso no TRE-PR, QRadar.

**2.2.1.44.39** - Deve gerar logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração.



**2.2.1.44.40** - Deverá ter a capacidade de gerar um relatório gráfico que permita visualizar as mudanças na utilização de aplicações na rede.

**2.2.1.44.41** - Emitir relatórios em tempo real para a visualização de origens e destinos do tráfego gerado na instituição.

**2.2.1.44.42** - Deve prover relatórios com visão correlacionada de aplicações, ameaças (IPS, *Antimalware* ou Antivírus e *Anti-spyware*), URLs e filtro de arquivos, para melhor diagnóstico e resposta a incidentes.

**2.2.1.44.43** - Deve permitir a criação de *Dash-Boards* customizados para visibilidades do tráfego de aplicativos, usuários, categorias de URL, ameaças identificadas pelo IPS, antivírus, *anti-spyware* (ou *anti-malware*), *malwares "Zero Day"* detectados em *sandbox* e tráfego bloqueado.

**2.2.1.44.44** - O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos dispositivos de segurança.

**2.2.1.44.45** - Dever permitir a visualização dos *logs* de *malwares* modernos, tráfego (IP de origem, destino, usuário e porta), aplicação, IPS, antivírus, *anti-spyware* (ou *anti-malware*), Filtro de URL e filtro de arquivos.

**2.2.1.44.46** - Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e *Anti-spyware* ou *Anti-malware*), etc..

**2.2.1.44.47** - Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus e *Anti-spyware* ou *anti-malware*), e URLs que passaram pela solução.

**2.2.1.44.48** - Deve possuir mecanismo "*Drill-Down*" para navegação nos relatórios em *Real Time*.

**2.2.1.44.49** - Nas opções de "*Drill-Down*", ser possível identificar o usuário que fez determinado acesso.

**2.2.1.44.50** - Deve possuir relatório de visibilidade e uso sobre aplicativos (SaaS). O relatório também deve mostrar os riscos para a segurança do ambiente, tais como a entrega de *malwares* por meio de aplicativos SaaS com a informação do usuário responsável pelo acesso.

**2.2.1.44.51** - Permitir a rotação dos logs.

**2.2.1.44.52** - Deve permitir que os logs e relatórios sejam rotacionados automaticamente baseado no tempo em que estão armazenados na solução, assim como no espaço em disco usado.

**2.2.1.44.53** - Exibição das seguintes informações, de forma histórica e em tempo real:

- a) Situação do dispositivo e do cluster;
- b) Principais aplicações;
- c) Administradores autenticados na gerência da plataforma de segurança;
- d) Status das interfaces;
- e) Uso de CPU;

**2.2.1.44.54** - No mínimo os seguintes relatórios devem ser gerados:

- a) Resumo gráfico de aplicações utilizadas;
- b) Principais aplicações por utilização de largura de banda de entrada e saída;

- c) Principais aplicações por taxa de transferência de bytes;
- d) Principais hosts por número de ameaças identificadas;
- e) Atividades de um usuário específico do AD/LDAP, incluindo aplicações acessadas, categorias de URL, e ameaças (IPS, Antivírus e *Anti-spyware* ou *anti-malware*), de rede vinculadas a este tráfego;
- f) Deve permitir a criação de relatórios personalizados.

**2.2.1.44.55** - Gerar alertas automáticos via, pelo menos, por e-mail e SNMP.

**2.2.1.44.56** - A plataforma de segurança deve permitir através de API (*Application Program Interface*) a integração com sistemas existentes no ambiente da contratante de forma a possibilitar que aplicações desenvolvidas na contratante possam interagir em Real Time com a solução possibilitando assim que regras e políticas de segurança de possam ser modificadas por estas aplicações com a utilização de scripts em linguagens de programação como Perl ou PHP.

**2.2.1.44.57** - Para comprovação de atendimento aos requisitos técnicos previstos neste termo **não** serão aceitas declarações e/ou cartas de fabricantes ou licitantes. Serão considerados os documentos de domínio público dos respectivos equipamentos e softwares. Caso a documentação de domínio pública seja omissa ou dúbia, poderá ser solicitada amostra para comprovação do atendimento das características (conforme item 9 do edital).

**2.2.1.44.58** - Os equipamentos ofertados devem obrigatoriamente ter certificação da ANATEL.

**2.2.1.44.59** - Caso a solução possua licenças relacionadas a armazenamento, deve ser ofertado a de capacidade ilimitada.

**2.2.1.44.60** - Caso a solução possua módulo de relatórios estendida, deverá ser entregue junto com a solução.

**2.2.1.44.61** - As licenças de atualização de software (firmware ou drivers) e licenças de atualização de assinaturas deverão ser fornecidas pelo prazo mínimo de 36 (trinta e seis) meses, a contar da data do recebimento definitivo dos produtos, sem ônus adicional para as atualizações e seu uso.

**2.2.1.44.62** - Garantia de 36 (trinta e seis) meses com envio de peças/equipamentos de reposição em até 3 (três) dias úteis, para todos os componentes da solução.

**2.2.2 – ITEM 2 – Licenças, garantia, suporte e atualizações por período adicional de 24 meses para toda a solução apresentada no item 1:**

**2.2.2.1** - Este item visa estender, por 24 meses, o funcionamento da solução de proteção de rede com características de Next Generation Firewall (NGFW) e da console de gerência, com todas as garantias de funcionamento do hardware, licenciamentos e respectivas assinaturas de serviço necessárias para seu funcionamento, incluindo, mas não se restringindo a:

**2.2.2.1.1** - Extensão do prazo de garantia da solução por 24 (vinte e quatro) meses, com envio de peças/equipamentos de reposição em até 3 dias úteis, para todos os componentes da solução;

**2.2.2.1.2** - Extensão do prazo de uso do serviço de atualização automática da base de classificação e categorização de aplicações conhecidas, sites e URLs, pelo período de 24 (vinte e quatro) meses;

**2.2.2.1.3** - Extensão do prazo de uso do serviço de atualização automática da base de assinaturas, utilizada pelo serviço de classificação e categorização de arquivos, pelo período de 24 (vinte e quatro) meses;

**2.2.2.1.4** - Extensão do prazo de atualizações das assinaturas do serviço de classificação e categorização de arquivos, pelo período de 24 (vinte e quatro) meses.

### **2.2.3 – ITEM 3 - Serviços de instalação, configuração e repasse de conhecimento.**

**2.2.3.1** - Os serviços de instalação, configuração e repasse de conhecimento deverão compreender, no mínimo, as seguintes atividades:

- a) Reunião para definição dos requisitos, arquitetura e topologia de instalação;
- b) Instalação física dos appliances em rack;
- c) Energização e conexão dos appliances em rede;
- d) Atualização de firmware dos appliances;
- e) Configuração das interfaces de gerenciamento;
- f) Ativação das licenças adquiridas;
- g) Configuração das interfaces de rede e regras de roteamento;
- h) Configuração dos objetos e regras de firewall e NAT;
- i) Ativação e configuração das funcionalidades de console de gerenciamento, URL Filter, controle de aplicação, VPN, prevenção contra ameaças, antivírus e malwares e sandbox;
- j) Migração de todo o ambiente atual para a nova solução
- k) Acompanhamento do processo de migração para a nova solução;
- l) Elaboração da documentação do ambiente implementado;
- m) Repasse de conhecimento, abordando o funcionamento geral da solução e a utilização da console de gerenciamento, com no mínimo 2 horas de duração.

**2.2.3.2** - Os serviços devem ser executados de segunda a sexta-feira, das 12 às 19 horas, na sede do TRE-PR.

**2.2.3.3** - A realização dos serviços deve ser planejada de acordo com disponibilidade de ambas as partes, em prazo máximo de 30 (trinta) dias após a entrega definitiva dos bens ou oficialização da ordem de empenho. O planejamento anterior ao serviço pode ser realizado remotamente através de webconferência ou videoconferência.

**2.2.3.4** - Ao término dos serviços deve ser criado um relatório detalhado contendo todos os itens configurados no projeto (as-built), etapas de execução e toda informação pertinente a posterior continuidade e manutenção da solução instalada.

**2.2.3.5** - Durante toda a implantação do projeto, o técnico da contratada deverá demonstrar aos técnicos da contratante como instalar e configurar os equipamentos e os softwares fornecidos (instalação assistida). Esta demonstração deverá contemplar os conceitos das tecnologias utilizadas pelo equipamento e a operação dos principais recursos dos produtos ofertados.

### **2.2.4 – ITEM 4 - Treinamento**

**2.2.4.1** - Voucher para treinamento oficial do fabricante, a ser ministrado pelo fabricante ou por um de seus parceiros credenciados.

**2.2.4.2** - A carga horária mínima do treinamento não poderá ser inferior a 32 (trinta e duas) horas;

**2.2.4.3** - O treinamento deverá ser realizado no Brasil, em português, contando com aulas teóricas e práticas.

**2.2.4.4** - O treinamento deve abordar, no mínimo:

- a) Principais funcionalidades;
- b) Configuração inicial;
- c) Configuração de políticas de segurança;
- d) Métodos de integração e autenticação de usuários;
- e) Configurações de NAT e QoS;
- f) Configurações de VPN (IPSec e SSL);
- g) Emissão e personalização de relatórios.

**2.2.4.5** - Deve ser emitido um certificado para cada servidor que participar da capacitação e tiver frequência mínima de 70% (setenta por cento).

**2.2.5 - Do suporte técnico durante a garantia contratual:**

**2.2.5.1-** Durante o período de Garantia , A CONTRATADA deverá prestar suporte técnico, atender às solicitações do TRE-PR, efetuadas pela Seção de Rede, respeitando as condições e níveis de serviço especificados a seguir;

**2.2.5.2-** A severidade dos chamados de suporte e garantia serão determinadas conforme este contrato e o prazo de atendimento será contado a partir da abertura de ordem de serviço e será classificado conforme as severidades especificadas a seguir;

**2.2.5.3-** Severidade ALTA: Esse nível de severidade é aplicado quando há indisponibilidade de componentes da solução ou as aplicações que são acessadas por meio da solução estão indisponíveis.

Dias úteis		Sábados, domingos e feriados	
Prazo de atendimento	Prazo de solução definitiva	Prazo de atendimento	Prazo de solução definitiva
06 horas	12 horas	08 horas	16 horas

**2.2.5.4-** Severidade MÉDIA: Esse nível de severidade é aplicado quando há falha no uso da solução, estando ainda disponível, porém apresentando problemas ou instabilidade.

Dias úteis		Sábados, domingos e feriados	
Prazo de atendimento	Prazo de solução definitiva	Prazo de atendimento	Prazo de solução definitiva
06 horas	48 horas	10 horas	48 horas

**2.2.5.5** - Severidade BAIXA: Esse nível de severidade é aplicado para a instalação, configuração, manutenções preventivas, aplicações de firmwares e esclarecimento técnico relativo ao uso da solução. Não haverá abertura de chamados de suporte técnico com esta severidade em sábados, domingos e feriados.

Dias úteis		Sábados, domingos e feriados	
Prazo de atendimento	Prazo de solução definitiva	Prazo de atendimento	Prazo de solução definitiva
30 horas	72 horas	-	-

**2.2.5.6-** Serão considerados para efeitos dos prazos exigidos:

**2.2.5.6.1.** Prazo de Atendimento: Tempo decorrido entre a solicitação efetuada pela Equipe Técnica do TRE-PR à Prestadora de Serviço e o efetivo início dos trabalhos de manutenção.

**2.2.5.6.2.** Prazo de Solução Definitiva: Tempo decorrido entre a solicitação efetuada pela Equipe Técnica do TRE-PR à Prestadora de Serviço e a efetiva recolocação dos equipamentos em seu pleno estado de funcionamento e operação normais.

**2.2.5.7 -** A contagem do prazo de atendimento e solução definitiva de cada solicitação será a partir da notificação à contratada, até o momento da comunicação da solução definitiva do problema e aceite pela equipe técnica do TRE-PR;

**2.2.5.8 -** O atendimento às solicitações de severidade ALTA deverá ser realizado nas instalações da TRE-PR (on-site) e não poderá ser interrompido até o completo restabelecimento do serviço, mesmo que se estenda para períodos noturnos, sábados, domingos e feriados. Nesse caso, não poderá implicar em custos adicionais ao TRE-PR. A interrupção do suporte técnico de uma solicitação desse tipo de severidade por parte da contratada e que não tenha sido previamente autorizado pelo TRE-PR, poderá ensejar na aplicação das sanções previstas neste contrato.

**2.2.5.9-** As ordens de serviços classificadas com severidade MÉDIA, quando não solucionados no prazo definido, poderão ser automaticamente escaladas para a severidade ALTA, sendo que os prazos de atendimento e solução definitiva do problema, bem como sanções previstas, serão automaticamente ajustados para o novo nível. A interrupção do suporte técnico de uma solicitação desse tipo de severidade por parte da contratada e que não tenha sido previamente autorizado pelo TRE-PR, poderá ensejar na aplicação das sanções previstas neste contrato.

**2.2.5.10-** Depois de concluído o suporte técnico, o licitante vencedor comunicará o fato à Equipe Técnica do TRE-PR e solicitará autorização para o fechamento do chamado. Caso o TRE-PR não confirme a solução definitiva do problema, o chamado permanecerá aberto até que seja efetivamente solucionado pela contratada. Nesse caso, o TRE-PR fornecerá as pendências relativas à solicitação em aberto.

**2.2.5.11-** O TRE-PR encaminhará a contratada, quando da reunião de apresentação inicial, relação nominal da equipe técnica autorizada a abrir e fechar solicitações de suporte técnico.



**2.2.5.12** - Por necessidade excepcional de serviço, o TRE-PR também poderá solicitar a escalção de chamado para níveis superiores de severidade. Nesse caso, a escalção deverá ser justificada e os prazos dos chamados passarão a contar do início novamente.

## **CLÁUSULA TERCEIRA: DAS OBRIGAÇÕES DA CONTRATADA**

### **3.1 – Da entrega:**

#### **3.1.1 – Do prazos:**

**3.1.1.1 – Prazo de entrega da solução:** a solução deverá ser entregue em um prazo de até **60 (sessenta) dias corridos**, a contar da assinatura do contrato.

**3.1.1.2 – Prazo de instalação e configuração:** a solução deverá ser instalada e configurada em um prazo de até **60 (sessenta) dias corridos**, contados da data de recebimento provisório.

**3.1.2 – Do local de entrega:** a solução deverá ser entregue no Tribunal Regional Eleitoral do Paraná, Rua João Parolin, nº 224, Curitiba-PR, Seção de Rede, agendamento pelos telefones (41) 3330-8628 ou 3330-8629.

### **3.2 - – Do recebimento do objeto:**

**3.2.1 – Do recebimento provisório:** em até 10 (dez) dias corridos a solução será recebida, provisoriamente, para efeito de posterior verificação de sua conformidade com as especificações constantes neste Termo de Referência.

**3.2.2 –** O recebimento provisório será realizado pela Seção de Gestão de Equipamentos de Microinformática.

**3.2.3 -** Na hipótese de constatação de anomalias que comprometam a utilização adequada da solução, ela será rejeitada, em todo ou em parte, conforme dispõe o Art. 76 da Lei nº 8.666/93, sem qualquer ônus para o TRE-PR, devendo o licitante vencedor reapresentá-la (s) no prazo máximo de até 30 (trinta) dias, após o comunicado.

**3.2.4 – Do recebimento definitivo:** a verificação da conformidade das especificações da solução ocorrerá no prazo de até 10 (vinte) dias corridos, contados a partir do recebimento provisório. Atestada a conformidade quantitativa e qualitativa, a solução será recebida definitivamente.

**3.2.4.1-** O recebimento definitivo será realizado pela Coordenadoria de Infraestrutura.

### **3.3 – Da garantia:**

**3.3.1 -** A solução ofertada deverá estar coberta por garantia total fornecida pelo fabricante, pelo prazo de **36 (trinta e seis) meses**.

**3.3.1.1 -** A garantia iniciará a partir da data de recebimento definitivo da solução.

**3.3.2** - A contratada deverá apresentar o Certificado de Garantia emitido pelo fabricante, no prazo de até 30 (trinta) dias corridos, a contar da data de recebimento definitivo da solução.

**3.3.3** - A contratada deverá possibilitar a abertura de chamado técnico diretamente no fabricante da solução ou por centro de suporte devidamente autorizado pelo fabricante.

**3.3.4** - O atendimento de primeiro nível deve ser realizado em português do Brasil.

**3.3.5** - Deve ser disponibilizado pelo menos um dos seguintes canais de atendimento para suporte:

- a) Telefone 0800;
- b) Sistema Web de abertura de chamados;
- c) E-mail.

**3.3.6** - A Contratada deverá disponibilizar o acesso direto à base de dados de conhecimento do fabricante da solução que contenha informações de assistência, orientação para instalação, desinstalação, configuração, atualização de *firmware e software*, aplicação de correções (patches), diagnóstico, avaliações e resolução de problemas, e demais atividades relacionadas à correta operação, e funcionamento da solução.

**3.3.7** - A Contratada deverá, semestralmente, revisar as atualizações de drivers, firmwares e microcódigos de todos os *appliances* contratados. Os serviços de atualizações de *firmwares* somente deverão ocorrer para os eventos classificados como críticos.

**3.3.8** - Os serviços cobertos pela garantia deverão ser prestados nas instalações do TRE-PR, em Curitiba/PR.

**3.3.9** - Os serviços cobertos pela garantia deverão ser prestados pela empresa fabricante, pela contratada ou parceiro autorizado/credenciado, através da disponibilização de técnicos certificados pelo fabricante da solução.

**3.3.10** - A Contratada deverá fornecer a seus técnicos as ferramentas e instrumentos necessários à execução dos serviços, bem como produtos ou materiais indispensáveis à manutenção do equipamento.

**3.3.11** - Os discos rígidos que forem substituídos ou no caso de troca de equipamento ficarão retidos e serão de propriedade do TRE-PR.

**3.3.12** - A Contratada deverá garantir atualizações do produto e suporte técnico do fabricante (telefone, e-mail ou acesso remoto) pelo período de vigência da garantia.

**3.3.13** - A substituição de equipamento defeituoso deverá ocorrer em até 30 (trinta) dias corridos, após a abertura de Ordem de Serviço pelo gestor de contrato ou notificação automática do sistema na central de atendimento do licitante vencedor ou fabricante.

**3.4** - A Contratada deverá apresentar, ao gestor da contratação, em até 30 (trinta) dias corridos contados da assinatura do contrato, no momento da entrega dos equipamentos, os documentos abaixo:

a) Certificação/declaração emitida pelo fabricante do equipamento ofertado (ou credenciado) para, no mínimo, 02 (dois) funcionários, atestando participação em

curso/treinamento específico relacionado à utilização/configuração/suporte do equipamento ofertado.

b) Comprovação do vínculo dos funcionários certificados (conforme alínea a) com a empresa contratada, mediante apresentação de carteira profissional ou contrato de prestação de serviços.

### 3.5 – Da sustentabilidade:

**3.5.1** - Será exigida a compatibilidade do produto com a diretiva RoHS (RoHS - Restriction of Certain Hazardous Substances ou Restrição de Certas Substâncias Perigosas), a qual limita a um percentual máximo o uso de substâncias perigosas nos processos de fabricação dos produtos, entre elas: cádmio (Cd), mercúrio (Hg), cromo hexavalente (CrVI), bifenilos polibromados (PBBs), éteres difenil-polibromados (PBDEs) e chumbo (Pb), de modo a contribuir para a redução do impacto ambiental.

**3.5.2** - Os produtos deverão ser preferencialmente, acondicionados em embalagem individual adequada, com menor volume possível, que utilize materiais recicláveis, de forma a garantir a máxima proteção durante o transporte e o armazenamento. As condições deste item serão objeto de verificação *in loco* no momento da entrega dos produtos.

**3.6** - A contratada obrigar-se-á em manter-se em compatibilidade com a habilitação e com as obrigações assumidas na licitação até o adimplemento total da contratação.

## CLÁUSULA QUARTA: DA DESPESA ORÇAMENTÁRIA

**4.1** – Os recursos serão destinados à contratação conforme abaixo:

Programa de Trabalho .....;  
Nota de Empenho: ....., emitida em ....../....../.....;  
Elemento de despesa: .....;  
Categoria Econômica: .....

## CLÁUSULA QUINTA: DA VIGÊNCIA

**5.1** - O presente contrato vigorará pelo período de **39 (trinta e nove) meses**, a partir da data da assinatura, **de .../.../..... a .../.../.....**, podendo ser rescindido antecipadamente a critério do CONTRATANTE, nos termos da lei nº 8.666/93.

## CLÁUSULA SEXTA: DO REAJUSTE

**6.1** - Os preços não serão reajustáveis, tendo em vista tratar-se de contrato de garantia contratual.

## CLÁUSULA SÉTIMA: DO PAGAMENTO

**7.1** - O valor total a ser pago à CONTRATADA, pelo cumprimento do objeto deste contrato será de **R\$..... (.....)**, conforme item(ns) a seguir especificado:

	Item	Descrição	Quantidade	Valor	Código siasg
LOTE 1	1	<i>Appliance Next Generation Firewall (NGFW)</i> , com interface de gerência e respectivas licenças, garantia, suporte e atualizações por 36 meses			BR0150100
	2	Licenças, garantia, suporte e atualizações por período adicional de 24 meses para toda a solução apresentada no item 1			24.333
	3	Serviços de instalação, configuração e repasse de conhecimento			22.128
	4	Treinamento			3840

## 7.2 – Do documento fiscal:

**7.2.1** – 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 por e-mail, em formato PDF ou emitido na forma física devendo ser encaminhado a Seção de Protocolo, localizada na Rua João Parolin, 224, 1º andar, Curitiba/Paraná.

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

**7.2.1.2** - 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 (CONTRATADA e eventual matriz ou filial utilizada) deverão estar com a documentação fiscal regular e atender obrigatoriamente os seguintes requisitos:

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

## 7.3 – Das condições do pagamento:

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

**7.3.2** - 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:

**7.3.2.1** – 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.

**7.3.2.1.1** - 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.

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

**7.3.2.2.1** - Se o valor da nota fiscal for de até R\$ 17.600,00 (dezesete mil e seiscentos reais), o prazo para pagamento será de **05 (cinco) dias úteis** após o atestado realizado pelo fiscal da contratação, conforme o disposto no art. 5º, § 3º da Lei nº 8.666/93.

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

**7.3.4** – O gestor da contratação do TRE/PR procederá à conferência dos requisitos da nota fiscal/fatura, que deverá estar de acordo com as descrições contidas na nota de empenho, bem como apresentar o mesmo número de CNPJ cadastrado, habilitado e constante nos documentos entregues, não se admitindo notas fiscais/faturas emitidas com outro CNPJ, salvo na hipótese prevista no item 7.2.1.2.

**7.3.4.1** – 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. Nessa hipótese, o prazo para pagamento iniciar-se-á após a regularização da situação, não acarretando qualquer ônus para o TRE/PR.

**7.3.5** – O TRE/PR, observados os princípios do contraditório e da ampla defesa, poderá deduzir, do montante a pagar à CONTRATADA, acréscimos decorrentes de mora no recolhimento de tributos/contribuições, bem como de multa decorrente de previsão deste edital e/ou anexo(s).

**7.3.6– DA ATUALIZAÇÃO MONETÁRIA:** Na ocorrência de eventual atraso de pagamento e, desde que a CONTRATADA não tenha concorrido para tanto, serão devidos encargos moratórios pelo TRE/PR, entre a data prevista para o pagamento e a do efetivo pagamento, mediante solicitação formal do interessado, que serão calculados por meio da aplicação da fórmula  $EM = I \times N \times VP$ , 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%)

$I = (6/100)/365$

## **7.4 – Da regularidade fiscal:**

**7.4.1** – 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.



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

**7.4.1.1.1** – Permanecendo a inadimplência poderá haver rescisão contratual, independentemente da aplicação das sanções previstas neste edital e/ou anexo(s).

**7.4.2** – A regularidade de que trata o subitem anterior poderá ser verificada:

- a) por meio de consulta on-line no Sistema de Cadastramento Unificado de Fornecedores - SICAF e/ou;
- b) por meio de consulta aos sites oficiais e/ou;
- c) por meio da apresentação de documentação, pela CONTRATADA, anexada ao documento fiscal.

**7.4.2.1** – O resultado das consultas, de que trata as alíneas acima, serão realizadas pelo setor financeiro responsável e deverão constar do processo de pagamento.

## **CLÁUSULA OITAVA: DA SUBSTITUIÇÃO TRIBUTÁRIA**

### **8.1 – Da substituição tributária:**

**8.1.1** - 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, LC nº 116/2003 e LC nº 123/06, conforme o objeto da contratação.

### **8.2 – Dos tributos federais:**

**8.2.1** - 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.

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

**8.2.3** - 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.

### **8.3 - Da retenção previdenciária:**

**8.3.1** - 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.

### **8.4 - Da retenção do ISS:**

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

**8.4.2** - 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).

**8.5** - 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.

**8.6** - A atualização monetária e a multa, provenientes do atraso no recolhimento das obrigações tributárias e/ou previdenciárias serão descontadas do valor da Nota Fiscal/Fatura correspondente, quando a CONTRATADA lhes der causa.

**8.6.1** - O não atendimento às especificações do documento fiscal, descritas na cláusula sétima, item 7.2, bem como a não comprovação da regularidade fiscal, prevista na cláusula sétima, item 7.4.1, darão causa ao previsto no item anterior.

## **CLÁUSULA NONA: DOS GESTORES DO CONTRATO**

**9.1** - O fornecimento será acompanhado pelo Chefe da Seção de Rede e seu substituto, que serão os gestores da contratação.

**9.2** - Nos termos da Lei nº 8666/93, art. 67, parágrafos 1º e 2º, caberá aos Gestores:

- a) receber e atestar a nota fiscal referente à aquisição, encaminhando a fatura pertinente ao setor responsável pelo tombamento dos bens e, seguidamente, à Secretaria de Orçamento, Finanças e Contabilidade do TRE/PR, para pagamento;
- b) acompanhar o fornecimento de acordo com as condições contratadas, determinando o que for necessário para regularização das faltas ou defeitos observados, sob pena de responsabilização administrativa;
- c) se a inexecução persistir, o gestor deverá criar um Processo Administrativo Digital (PAD) específico e encaminhá-lo à Secretaria de Gestão Administrativa, devidamente instruído com todas as informações pertinentes constantes de formulário específico, anexando-se cópia(s) do(s) e-mail(s) relativos ao item anterior (letra “b”), referente(s) à intenção de abertura de Processo Administrativo, com o respectivo comprovante de recebimento pela Contratada.

## **CLÁUSULA DÉCIMA: DAS SANÇÕES ADMINISTRATIVAS**

**10.1** - O descumprimento de quaisquer das obrigações descritas no presente instrumento poderá ensejar abertura de processo administrativo, garantido o contraditório e a ampla defesa, de acordo com o capítulo IV, art. 87 da Lei nº 8666/93 e artigo 7º da lei nº 10520/2002:

**10.2** – Poderão ser aplicadas ainda as seguintes sanções:

a) Advertência;

b) Multas:

b.1) Multa de 1,0% (um por cento) ao dia sobre o valor contratado, pelo atraso no cumprimento ao prazos de entrega estipulado no presente instrumento, com limite de 10 (dez) dias. Após esse prazo, será considerado inadimplemento parcial, com multa de 15% (quinze por cento) sobre o valor total do contrato;

b.2) Multa de 5,0% (cinco por cento) sobre o valor total da contratação pelo inadimplemento a quaisquer outras obrigações pactuadas, e que venham a causar prejuízos o CONTRATANTE, independente do ressarcimento dos danos à

Administração.

b.3) Na prestação da Garantia Técnica, estará sujeita às sanções abaixo, pelos descumprimentos dos prazos previstos para solucionar os chamados de SUPORTE TÉCNICO, nos termos previstos no item 2.3 deste contrato, conforme abaixo:

Sanção	Classificação
0,05 % por dia de atraso, limitado a 30 dias , sobre o valor total do contrato.	Severidade alta
0,02% por dia de atraso , limitado 30 dias , sobre o valor total do contrato.	Severidade média
0,01% por dia de atraso , limitado a 30 dias , sobre o valor total do contrato.	Severidade baixa

b.4) Multa de 10% (dez por cento) sobre o valor total do contrato, pela não prestação da garantia dos equipamentos e/ou serviços fornecidos dentro dos prazos previstos em contrato e/ou no Código de Defesa do Consumidor; ou pela ocorrência de quaisquer danos aos equipamentos, ocasionados por negligência ou imperícia dos profissionais, sem a reposição ou conserto imediato do bem pertinente;

b.5) Multa de 15% (quinze por cento) sobre o valor total do contrato, pela não atendimento a qualquer chamado feito pelo CONTRATANTE para manutenção e correção de problemas ou pela inadimplência reiterada das obrigações pactuadas.

b.6) Multa de 10% (dez por cento) sobre o valor contratual, pelo inadimplemento parcial do contrato;

b.7) Multa de 20% (vinte por cento) sobre o valor contratual, pelo inadimplemento total do contrato;

c) Impedimento de licitar e contratar com a União, conforme previsto no art.7º da Lei nº 10.520/2002, 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 10.520/2002, pelo prazo de até 05 (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 prejuízos ocasionados, 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.

**10.4** - As sanções de advertência e de impedimento de licitar e contratar, previstas nos itens 10.1, 10.2 , poderão ser aplicadas, cumulativamente ou não, com a pena de multa.

**10.5** - No caso de aplicação de multa determinada em processo administrativo que garanta a ampla defesa à CONTRATADA, esta deverá recolher à União o valor imputado por meio de GRU.

**10.6** - As multas imputadas à Contratada cujo montante seja superior ao mínimo

estabelecido pelo Ministério da Fazenda<sup>2</sup> e não pagas no prazo concedido pela Administração, serão inscritas em Dívida Ativa da União e cobradas com base na Lei nº 6830/80, sem prejuízo da correção monetária pelo IGP-M ou outro índice que porventura venha a substituí-lo.

#### **CLÁUSULA DÉCIMA PRIMEIRA: DA RESCISÃO DO CONTRATO**

**11.1** - Ficarão o presente contrato rescindido, a juízo da administração, mediante formalização, assegurado o contraditório e a ampla defesa, nos casos elencados nos arts. 77 a 80 da Lei nº 8.666/93.

**11.2** - 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, 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).

#### **CLÁUSULA DÉCIMA SEGUNDA: DOS CASOS OMISSOS**

**12.1** - 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 TERCEIRA: DO FORO**

**13.1** - Fica eleito o Foro de Curitiba-PR para dirimir as divergências oriundas do presente contrato.

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

Curitiba, .... de ..... de 201...

.....  
Representante Legal  
P/ CONTRATADA

**Valcir Mombach**  
Diretor-Geral - TRE/PR.  
P/ CONTRATANTE

<sup>2</sup> Portaria n.º 75 do Ministério da Fazenda, publicada em 22/03/2012 – artigo 1.º, inciso I.