



TRIBUNAL REGIONAL ELEITORAL DO PARA

EDITAL DE LICITAÇÃO Nº 46/2022

PREGÃO ELETRÔNICO (Proc. Prot. n.º 0008981-46.2021.6.14.8000)				
ATENÇÃO <p>No Acórdão TCU nº 754/2015 – Plenário, há expressa determinação para que a Administração Pública instaure processo com vista à penalização das empresas que pratiquem, injustificadamente, ato tipificado no art. 7º da Lei nº 10.520/2002, tanto na licitação quanto no contrato.</p> <p>Nesse contexto, alerta-se para que as empresas licitantes analisem detalhadamente o Edital (e Anexos), de modo a formular propostas / lances consistentes e passíveis de cumprimento.</p> <p>A prática injustificada de atos como: não manter a proposta (ex.: desistência, solicitação de troca de marca / modelo, não envio de amostra, planilha, laudos) e deixar de enviar documentação exigida (ex.: documentos de habilitação), sem prejuízo de outras infrações cometidas na licitação / contratação, sujeitará a licitante a eventual aplicação de penalidade, apurada em processo administrativo específico.</p>				
OBJETO				
REGISTRO DE PREÇOS DE SOLUÇÃO DE WEB APPLICATION FIREWALL (WAF) E BALANCEAMENTO DE CARGA, INCLUINDO PRESTAÇÃO DE SERVIÇOS DE INSTALAÇÃO E CONFIGURAÇÃO, TREINAMENTO ESPECIALIZADO E SERVIÇO DE OPERAÇÃO ASSISTIDA, COM GARANTIA TÉCNICA DE 60 (SESENTA) MESES, de acordo com as características mínimas descritas no Anexo I - Termo de Referência.				
VALOR TOTAL ESTIMADO: R\$ 41.688.680,97 (quarenta e um milhões, seiscentos e oitenta e oito mil, seiscentos e oitenta reais e noventa e sete centavos)				
DATA: 25/07/2022 HORÁRIO: 9h (horário de Brasília) ENDEREÇO ELETRÔNICO: https://www.gov.br/compras/pt-br UASG: 070004				
Registro de Preços?	Tipo:	Lançamentos de Sistema:	Exclusiva ME/EPP?	Reserva de cota exclusiva ME/EPP?
SIM	Menor preço	Proposta: Vide item 4.2 do Edital Lances: Vide item 7.2 do edital.	NÃO	NÃO
Critério de Julgamento		Decreto nº 7.174/2010?	Apresentação de amostra?	Vistoria prévia?
Menor Preço Global por Lote		SIM	NÃO	NÃO
Pedidos de Esclarecimentos e Impugnações				
Até 3 dias úteis anteriores à data fixada para abertura da sessão pública, qualquer pessoa poderá impugnar o presente ato convocatório, exclusivamente por meio eletrônico, via internet, nos seguintes				

endereços: pregoeiros@tre-pa.jus.br, coinf@tre-pa.jus.br e selic@tre-pa.jus.br.

Os pedidos de esclarecimento referentes ao presente Edital serão enviados ao Pregoeiro, até **03 dias úteis** anteriores à data fixada para abertura da sessão pública, exclusivamente por meio eletrônico, via internet, nos seguintes endereços: pregoeiros@tre-pa.jus.br, coinf@tre-pa.jus.br e selic@tre-pa.jus.br.

Documentos de Habilitação

Documentação SICAF: Item 11.3 do Edital

Documentação Complementar: Item 11.4 do Edital

ANEXOS

- a) Anexo I – Termo de Referência;
- b) anexo II - Minuta da Ata de Registro de Preços.
- c) Anexo III - Minuta de Contrato

O Tribunal Regional Eleitoral do Pará, por intermédio de **DILSON ATHIAS MESQUITA**, Pregoeiro designado pela **Portaria nº 8.685/2007**, torna público, para conhecimento dos interessados, que na data, horário e endereço eletrônico abaixo indicados, fará realizar **licitação, na modalidade PREGÃO, forma ELETRÔNICA, tipo MENOR PREÇO**, em sessão pública virtual, por meio da INTERNET, mediante condições de segurança – criptografia e autenticação – em todas as suas fases, da seguinte forma:

PRINCIPAIS NORMAS APLICÁVEIS:

- **Lei nº 10.520/2002** (Institui a modalidade de licitação denominada Pregão);
- **Lei Complementar nº 123/2006** (Institui o Estatuto Nacional da Microempresa e da Empresa de Pequeno Porte);
- LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);
- **Decreto nº 3.555/2000** (Regulamento do pregão);
- **Decreto nº 7.892/2013** (Regulamenta o Sistema de Registro de Preços);
- **Decreto nº 8.538/2015** (Regulamenta o tratamento favorecido, diferenciado e simplificado para as microempresas, empresas de pequeno porte...);
- **Decreto nº 10.024/2019** (Regulamenta o pregão na forma eletrônica);
- **Decreto nº 9.507/2018** (Dispõe sobre a execução indireta, mediante contratação, de serviços da administração pública federal direta, autárquica e fundacional e das empresas públicas e das sociedades de economia mista controladas pela União);
- **Lei nº 8.248/1991 e Decreto nº 7.174/2010** (Regulamenta a contratação de bens e serviços de informática e automação);
- **Resolução do Conselho Nacional de Justiça nº 182/2013** (Dispõe sobre diretrizes para as contratações de Solução de Tecnologia da Informação e Comunicação);
- **Resolução CNJ 370/2021** (Estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário - ENTIC-JUD);
- Resolução CNJ nº 396, de 7 de junho de 2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);
- Resolução TSE Nº 23.644, de 1º de julho de 2021, Dispõe sobre a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;
- **Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019** (Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal);
- **Portaria TRE-PA nº 18456/2019** (Estabelece as diretrizes para a Gestão de Ativos de Tecnologia da Informação e Comunicações e institui o processo de gestão de configuração e ativos de TIC no âmbito do TRE-PA).

Subsidiariamente:

- **Lei nº 8.666/1993** (Lei de Licitações e Contratações da Administração Pública);
- **Decreto nº. 3.722/2001 e Instrução Normativa SEGES/MPGD nº 03/2018** (Sistema de Cadastramento Unificado de Fornecedores – SICAF).

1 - DO OBJETO

1.1. A presente licitação tem por objeto o **REGISTRO DE PREÇOS DE SOLUÇÃO DE WEB APPLICATION FIREWALL (WAF) E BALANCEAMENTO DE CARGA, INCLUINDO PRESTAÇÃO DE SERVIÇOS DE INSTALAÇÃO E CONFIGURAÇÃO, TREINAMENTO ESPECIALIZADO E SERVIÇO DE OPERAÇÃO ASSISTIDA, COM GARANTIA TÉCNICA DE 60 (SESSENTA) MESES**, de acordo com as características mínimas descritas no Anexo I - Termo de Referência.

1.2. Os **bens e serviços** deverão atender às normas do Código de Defesa do Consumidor.

1.3. Caso as especificações deste objeto encontrem-se discordantes no Compras governamentais e neste Edital, prevalecerão as constantes deste.

2 - DAS CONDIÇÕES DE PARTICIPAÇÃO

2.1. Poderão participar deste Pregão os interessados cujo ramo de atividade seja compatível com o objeto desta licitação e que estejam previamente credenciados no Sistema de Cadastramento Unificado de Fornecedores - SICAF e no Sistema de Compras do Governo Federal - este último disponível no endereço eletrônico <https://www.gov.br/compras/pt-br>.

2.1.1. A licitante responsabilizar-se-á exclusiva e formalmente pelas transações efetuadas em seu nome, assumindo como firmes e verdadeiras suas propostas e seus lances, inclusive os atos praticados diretamente ou por seu representante, excluída a responsabilidade do provedor do sistema ou do órgão ou entidade promotora da licitação por eventuais danos decorrentes de uso indevido das credenciais de acesso, ainda que por terceiros.

2.2. A comprovação da regularidade fiscal e trabalhista, da qualificação econômico-financeira e da habilitação jurídica, conforme o caso, dar-se-á primeiramente por meio de consulta ao cadastro no SICAF;

2.2.1. O cadastramento no SICAF observará as disposições da Instrução Normativa SEGES/MPDG nº 03/2018 e contera os registros da habilitação jurídica, da regularidade fiscal e da qualificação econômico-financeira, bem como das sanções aplicadas pela Administração Pública, conforme previsto na legislação e na Instrução Normativa acima referenciada, em especial as que acarretam a proibição de participação em licitações e celebração de contratos com o Poder Público.

2.3. Como requisito para participação neste Pregão, a licitante declarará, em campo próprio do sistema, o cumprimento dos requisitos de habilitação e a conformidade de sua proposta com as exigências do Edital.

2.3.1. Para comprovação do pleno conhecimento e atendimento das exigências de habilitação, a licitante deverá registrar, no Sistema COMPRASGOVERNAMENTAIS, o cumprimento do inteiro teor dos seguintes documentos:

a) **Declaração ME/EPP/COOP** (Declaração de Microempresa, Empresa de Pequeno Porte, nos termos da Lei Complementar nº 123, de 2006), se for o caso;

b) **Declaração de Ciência - Edital** (Declaração de que está ciente e concorda com as condições contidas no ato convocatório e seus anexos, bem como de que cumpre plenamente os requisitos de habilitação definidos no referido documento);

c) **Declaração de Cumprimento dos requisitos de habilitação e conformidade da proposta** (Declaração de que cumpre os requisitos para a habilitação definidos no Edital e que a proposta apresentada está em conformidade com as exigências editalícias - Decreto nº 10.024/2019);

d) **Declaração - Fato Superveniente** (Declaração, sob as penas da lei, de que até a presente data inexistem fatos impeditivos para a sua habilitação no presente processo licitatório, ciente da obrigatoriedade de declarar ocorrências posteriores);

e) **Declaração de Menor** (Declaração, para fins do disposto no inciso V do art. 27 da Lei nº 8.666 de 1993, acrescido pela Lei nº 9.854, de 27 de outubro de 1999, de que não emprega menor de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 (dezesesseis) anos, salvo menor a partir de 14 (quatorze) anos, na condição de aprendiz, nos termos do inciso XXXIII do art. 7º da Constituição Federal);

f) **Declaração Independente de Proposta** (Declaração de que a proposta apresentada para essa licitação foi elaborada de maneira independente);

g) **Declaração de Não Utilização de Trabalho Degradante ou Forçado** (Declaração de que não possui, em sua cadeia produtiva, empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal);

b) **Declaração de Acessibilidade** (Declaração de que cumpre o disposto no art. 93 da Lei nº 8.213, de 24 de julho de 1991, que determina a reserva de cargos para pessoas com deficiência ou para reabilitados da Previdência Social que atendam às regras de acessibilidade previstas na legislação);

i) **Declaração de Cota de Aprendizagem** (Declaração de que cumpre com o disposto no art. 429 da CLT, que determina aos estabelecimentos de qualquer natureza que empreguem e matriculem nos cursos dos Serviços Nacionais de Aprendizagem número de aprendizes equivalente a cinco por cento, no mínimo, e quinze por cento, no máximo, dos trabalhadores existentes em cada estabelecimento, cujas funções demandem formação profissional).

2.4. A declaração falsa relativa ao cumprimento dos requisitos de habilitação e aceitação da proposta sujeitará a licitante às sanções previstas neste Edital.

2.5. Não poderão participar deste Pregão:

a) os interessados que se encontrem em processo de falência, recuperação judicial ou extrajudicial, concordata, concurso de credores, dissolução ou liquidação, observado o disposto no item 2.5.1;

b) interessados reunidos em regime de consórcio, qualquer que seja sua forma de constituição;

c) empresas estrangeiras não autorizadas a funcionar no país;

d) empresas declaradas inidôneas, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida sua reabilitação (art. 87, IV da Lei nº 8.666/93);

e) empresas suspensas ou impedidas de licitar e/ou contratar com o TRE/PA, durante o prazo da sanção aplicada (art. 87, III da Lei nº 8.666/93);

f) empresas impedidas de licitar e contratar com a União (art. 7º da Lei nº 10.520/02);

g) quaisquer interessados que se enquadrem nas vedações previstas no art. 9º, da Lei nº 8.666/93;

h) empresário proibido de contratar com o Poder Público, nos termos do art. 12 da Lei nº 8.429/92;

i) empresário proibido de contratar com o Poder Público, em razão do disposto no art. 72, § 8º, V, da Lei nº 9.605/98.

2.5.1. Excepcionalmente, será admitida a participação de empresas em recuperação judicial que comprovem o acolhimento judicial de seu plano de recuperação, na forma do art. 58 da Lei 11.101, de 2005, ou estejam amparadas em certidão emitida pela instância judicial competente afirmando que a interessada está apta econômica e financeiramente a participar de procedimento licitatório (**Acórdão TCU 1201/2020 - Plenário**), devendo, ainda, comprovar todos os demais requisitos de habilitação. Nestes casos, os atos, contratos e documentos firmados terão acrescidos, após o nome empresarial, a expressão "em Recuperação Judicial", conforme art. 69 do referido diploma legal.

2.6. A licitante está obrigada a declarar, no sistema eletrônico, sua condição, ou não, de Empresa de Pequeno Porte - EPP, Microempresa – ME ou sociedade cooperativa que tenha auferido, no ano-calendário anterior, receita bruta até o limite definido no caput do art. 3º da Lei Complementar nº 123/2006 e alterações e art. 34 da Lei nº 11.488/2007.

2.7. Para esta licitação não haverá exclusividade para microempresas e empresas de pequeno porte, tendo em vista o valor médio obtido em pesquisa de mercado (coleta de preços).

3 - DO CREDENCIAMENTO

3.1. A licitante deverá credenciar-se no sistema “Pregão Eletrônico”, no sítio <https://www.gov.br/compras/pt-br>, observado o seguinte:

a) o credenciamento far-se-á mediante atribuição de chave de identificação e de senha, pessoal e intransferível, para acesso ao sistema eletrônico;

b) a perda da senha ou a quebra de sigilo deverão ser comunicadas imediatamente ao provedor do sistema para imediato bloqueio de acesso;

c) o credenciamento da licitante ou de seu representante perante o provedor do sistema implicará responsabilidade legal pelos atos praticados e presunção de sua capacidade técnica para realização das transações inerentes ao pregão eletrônico.

3.2. 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 órgão promotor da licitação responsabilidade por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros.

3.3. A licitante responsabilizar-se-á por todas as transações que forem efetuadas em seu nome no sistema eletrônico, assumindo como firme e verdadeira sua proposta, assim como os lances inseridos durante a sessão pública.

4 – DO ENCAMINHAMENTO DA PROPOSTA DE PREÇOS E DOS DOCUMENTOS DE HABILITAÇÃO

4.1. Após a divulgação do Edital, a licitante deverá encaminhar, até a data e hora marcadas para a abertura da sessão, exclusivamente por meio eletrônico, **concomitantemente com os documentos de habilitação exigidos no Edital**, proposta de preços com os respectivos Anexos, se for o caso, **formulada de acordo com o termo de referência**, atentando para as especificações detalhadas do objeto, quando, então, encerrar-se-á, automaticamente, a fase de recebimento dessa documentação.

4.1.1. O envio da proposta, acompanhada dos documentos de habilitação exigidos neste Edital, ocorrerá por meio de chave de acesso e senha.

4.1.2. As Microempresas e Empresas de Pequeno Porte deverão encaminhar a documentação de habilitação, ainda que haja alguma restrição de regularidade fiscal e trabalhista, nos termos do art. 43, § 1º da LC nº 123, de 2006.

4.1.3. Até a abertura da sessão pública, as licitantes poderão retirar ou substituir a proposta e os documentos de habilitação anteriormente inseridos no sistema;

4.1.4. Não será estabelecida, nessa etapa do certame, ordem de classificação entre as propostas apresentadas, o que somente ocorrerá após a realização dos procedimentos de negociação e julgamento da proposta.

4.1.5. Os documentos que compõem a proposta e a habilitação da licitante melhor classificada somente serão disponibilizados para avaliação do pregoeiro e para acesso público após o encerramento do envio de lances.

4.1.6. Qualquer elemento que possa identificar a licitante, antes do encerramento da fase de lances, importará a desclassificação da proposta.

4.2. A licitante deverá consignar, obrigatoriamente, em campo adequado do sistema eletrônico, os valores unitários dos itens, devendo respeitar os valores máximos unitários e globais para cada item que compõe o LOTE, indicados no Item 4.7 do Anexo I – Termo de Referência, não podendo ser aceitas pelo(a) pregoeiro(a) propostas com valores acima dos previstos pela Administração.

4.2.1. Para os lançamentos das propostas no sistema devem ser adotados os seguintes parâmetros:

a) No campo "VALOR UNITÁRIO ": Registrar o valor unitário de cada item que compõe o lote – Letra "B" da tabela constante do Item 4.7 do Anexo I – Termo de Referência;

b) No campo "QUANTIDADE": Informar a quantidade de itens a serem fornecidos, de acordo com cada item a ser registrado – Letra "A" da tabela constante do Item 4.7 do Anexo I – Termo de Referência.

4.2.2. Os preços apresentados devem abranger todos os os custos diretos e indiretos, tributos, taxas de administração, materiais, serviços, encargos sociais, trabalhistas, seguros, lucros e outros necessários ao cumprimento integral do objeto.

4.3. A licitante deverá preencher o campo com a descrição detalhada do objeto ofertado e todas as informações necessárias para aferir que o material ofertado atende às exigências do Edital, evitando a pura transcrição do disposto no termo de referência.

4.4. A proposta da licitante deverá vir acompanhada de documentação técnica que comprove o atendimento de todos os requisitos do termo de referência. Para tal, deverá ser indicado na proposta comercial os part number(s) referente(s) (PartNumbers/SKUs) a cada software(s) fornecido(s), licenças de uso e garantia do produto. Adicionalmente, **a licitante deverá indicar, ponto a ponto, qual seção da documentação técnica comprova o atendimento de cada requisito e conformidade do material proposto** com a especificação exigida no termo de referência, evitando a pura transcrição do disposto no Termo de Referência para a proposta;

4.5. A LICITANTE deverá indicar em sua proposta os fabricantes, modelos e versões de todos os componentes das soluções, incluindo componentes de hardware (se houver) e de software, realizando a indicação de todos os Códigos de Produto. Devem ser entregues prospectos/folders/folhetos com as características técnicas dos equipamentos, softwares e licenças. Devem ser apresentadas, de forma clara e detalhada, as descrições das soluções com todos os seus componentes (hardware e software), podendo ser complementadas por documentações integrantes da proposta, tais como: brochuras, catálogos, manuais técnicos, manuais de operação, etc. Na especificação técnica devem ser destacados e referenciados pelo licitante os requisitos mínimos exigidos no Termo de Referência, com a indicação do documento e página onde se encontra grifada a comprovação, sob pena de desclassificação;

4.6. A LICITANTE garantirá que o bem, quer seja de sua fabricação ou integralmente ou parcialmente de subfornecedores, estará exatamente de acordo com estas especificações, isentos de defeitos de fabricação, de matéria prima ou mão de obra. Deverá, também, ser informado o prazo de garantia, conforme especificado neste Termo de Referência;

4.7. Não será aceita oferta de objeto com especificações diferentes das indicadas nos Anexos deste Edital.

4.8. Os valores deverão ser propostos com duas casas decimais.

4.9. A proposta apresentada em desacordo com este Edital será desclassificada.

- 4.10. É obrigatória a apresentação de propostas para todos os itens que compõem o lote.
- 4.11. As propostas terão validade de 60 (sessenta) dias, contados da data de abertura da sessão pública estabelecida no preâmbulo deste Edital.
- 4.12. As licitantes poderão deixar de apresentar os documentos de habilitação que constem do SICAF, assegurado aos demais licitantes o direito de acesso aos dados constantes dos sistemas.
- 4.13. Decorrido o prazo de validade das propostas, sem convocação para assinatura da Ata de Registro de Preços, ficam as licitantes liberadas dos compromissos assumidos.

5 – DA ABERTURA DA SESSÃO PÚBLICA

- 5.1. No dia e hora indicados no preâmbulo deste Edital, o pregoeiro abrirá a sessão pública na internet, mediante a utilização de sua chave de acesso e senha, no sítio <https://www.gov.br/compras/pt-br>.
- 5.2. A comunicação entre o pregoeiro e as licitantes ocorrerá exclusivamente mediante troca de mensagens, em campo próprio do sistema eletrônico.
- 5.3. As propostas de preços contendo a descrição do objeto, o valor e os eventuais Anexos estarão disponíveis na internet.
- 5.4. Após a abertura, o pregoeiro verificará as propostas apresentadas, desclassificando aquelas que não apresentarem conformidade com os requisitos estabelecidos neste Edital.
- 5.5. Cabe à licitante acompanhar as operações no sistema eletrônico durante a sessão pública do Pregão, ficando responsável pelo ônus decorrente da perda de negócios diante da inobservância de qualquer mensagem emitida pelo sistema ou de sua desconexão.

6 – DA CLASSIFICAÇÃO DAS PROPOSTAS

- 6.1. O(A) Pregoeiro(a) verificará as propostas apresentadas e desclassificará, motivadamente, aquelas que não estiverem em conformidade com os requisitos estabelecidos neste Edital, registrando no sistema, com acompanhamento, em tempo real, por todos os participantes.
- 6.1.1. A desclassificação de um item implicará na desclassificação de todo o lote.
- 6.2. Somente as licitantes com propostas classificadas participarão da fase de lances.

7 – DA FORMULAÇÃO DOS LANCES

- 7.1. Aberta a etapa competitiva, as licitantes classificadas poderão encaminhar lances, exclusivamente por meio do sistema eletrônico, sendo imediatamente informadas do recebimento e respectivo horário de registro e valor.
- 7.2. Na formulação de lances, deverão ser observados os seguintes aspectos:
- a) os lances deverão ser ofertados pelo valor unitário de cada item que compõe o lote;**
- b)** as licitantes deverão ofertar lances com duas casas decimais, caso contrário o (a) Pregoeiro (a) não os aceitará;
- c)** as licitantes poderão oferecer lances sucessivos, observados o horário fixado para abertura da sessão e as regras estabelecidas neste Edital;
- d)** não serão aceitos dois ou mais lances iguais, prevalecendo aquele que for recebido e registrado primeiramente;
- e)** o intervalo entre os lances enviados pela mesma licitante não poderá ser inferior a 20 segundos, sob pena de serem descartados automaticamente pelo sistema.
- 7.3. Durante a sessão pública deste pregão, as licitantes serão informadas, em tempo real, do valor do menor lance registrado, vedada a identificação da ofertante.
- 7.4. Os lances apresentados e levados em consideração para efeito de julgamento serão de exclusiva e total responsabilidade da licitante, não lhe cabendo o direito de pleitear qualquer alteração.
- 7.5. Nesta fase, o pregoeiro poderá excluir, justificadamente, lance de valor considerado inexequível.
- 7.6. Será adotado para o envio de lances no pregão eletrônico o modo de disputa “aberto e fechado”, em que as licitantes apresentarão, na fase aberta, lances públicos e sucessivos, com lance final e fechado, na fase sigilosa.
- 7.7. A etapa de lances, na fase aberta, terá duração inicial de 15 minutos.
- 7.7.1. Encerrado o prazo acima, o Sistema enviará aviso de fechamento iminente de lances e, após transcorrido período de até 10 minutos, aleatoriamente determinado pelo sistema, encerrará automaticamente a recepção de lances.
- 7.7.2. Findo o prazo acima, o Sistema abrirá a oportunidade para que o autor do menor lance e os autores das ofertas com valores até 10% superiores àquela possam ofertar um lance final e fechado em até 5 minutos.

7.8. Na ausência de, no mínimo, 3 ofertas na condição definida no item 7.7.2, os autores dos melhores lances subsequentes, na ordem de classificação, até o máximo de 3, poderão oferecer um lance final e fechado, em até 5 minutos.

7.9. Na ausência de lance final e fechado, haverá o reinício da etapa fechada para que as demais licitantes, até o máximo 3, na ordem de classificação, possam ofertar um lance final e fechado, em até 5 minutos.

7.10. O lance final e fechado previsto nos itens 7.7.2, 7.8 e 7.9 será sigiloso até o encerramento do prazo de 5 minutos.

7.10.1. Encerrados os prazos previstos nos itens 7.7.2, 7.8 e 7.9 o Sistema ordenará os lances em ordem crescente de vantajosidade.

7.11. Na hipótese de não haver licitante classificada na etapa de lance fechado que atenda às exigências de habilitação, o Pregoeiro poderá, auxiliado pela equipe de apoio, mediante justificativa, reiniciar a etapa fechada, nos termos do item 7.7.2.

7.12. O sistema, automaticamente, assegurará às Empresas de Pequeno Porte - EPP, Microempresas – ME ou sociedades cooperativas que tenham auferido, no ano-calendário anterior, receita bruta até o limite definido no caput do art. 3º da Lei Complementar nº 123/2006 e alterações e art. 34 da Lei nº 11.488/2007, a preferência de desempate quando o preço por elas ofertado for igual ou até 5% superior ao melhor preço registrado por empresa que não se encontre nesta caracterização (art. 44, § 2º da Lei Complementar nº 123/2006).

7.12.1. Neste caso, após o encerramento dos lances, o sistema concederá o prazo de 5 (cinco) minutos, sob pena de preclusão, para a microempresa, a empresa de pequeno porte ou sociedade cooperativa, acima referida, apresentar proposta de preço inferior àquela considerada vencedora.

7.12.2. No caso de equivalência dos valores apresentados pelas microempresas, empresas de pequeno porte ou sociedades cooperativas, referidas no item 7.12, que se encontrem no intervalo acima informado (5%), o sistema realizará sorteio entre elas para que se identifique aquela que primeiro poderá apresentar a melhor oferta.

7.13. O disposto no item 7.12 somente se aplicará quando a melhor oferta inicial não tiver sido apresentada por microempresa, empresa de pequeno porte ou sociedade cooperativa, referida no item 7.12 (art. 45, §2º da Lei Complementar nº 123/2006).

7.14. Não será admitida a desistência da proposta/lance, após o início da fase de lances, bem como após o seu encerramento.

7.14.1. Excepcionalmente, após o encerramento da fase de lances, poderá ser acatado o pedido de desistência da proposta, em razão de motivo justo devidamente comprovado pela licitante, decorrente de fato superveniente, a ser analisado pelo(a) Pregoeiro(a).

7.14.2. O(A) pregoeiro(a) decidirá, motivadamente, acerca do pedido. Caso não seja aceito e a licitante mantiver a intenção de desistência, o(a) pregoeiro(a) examinará a proposta subsequente, na forma do item **10.4** do Edital, ficando a licitante desistente sujeita a aplicação das sanções previstas no item **19 deste Edital**, em procedimento a ser instaurado, resguardando-se o seu direito ao contraditório e ampla defesa.

7.15. Havendo eventual empate entre propostas iguais não seguidas de lances, ou entre lances finais da fase fechada do modo de disputa aberto e fechado, será aplicado o critério de desempate previsto no item 7.12.

7.15.1. Não sendo aplicável o disposto no item 7.12 deste Edital, o critério de desempate será aquele previsto no art. 3º, § 2º, da Lei nº 8.666, de 1993, assegurando-se a preferência, sucessivamente, aos bens produzidos:

- a) no país;
- b) por empresas brasileiras;
- c) por empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País;
- d) por empresas que comprovem o cumprimento de reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social e que atendam às regras de acessibilidade previstas na legislação.

7.16. Persistindo o empate, a proposta vencedora será sorteada pelo sistema eletrônico dentre as propostas empatadas.

7.17. Será assegurada, ainda, preferência na contratação nos termos do disposto no art. 3º, da Lei nº 8.248/1991, regulado pelo art. 5º do Decreto nº 7.174/2010, observada a seguinte ordem:

I - bens e serviços com tecnologia desenvolvida no País e produzidos de acordo com o Processo Produtivo Básico (PPB), na forma definida pelo Poder Executivo Federal;

II - bens e serviços com tecnologia desenvolvida no País; e

III - bens e serviços produzidos de acordo com o PPB, na forma definida pelo Poder Executivo Federal.

7.18. O exercício do direito de preferência para fornecedores de bens e serviços disposto no item 7.17 será concedido observando-se os seguintes procedimentos, sucessivamente:

- a) aplicação das regras de preferência previstas no item 7.17, com classificação dos licitantes cujas propostas finais estejam situadas até 10% (dez por cento) acima da melhor proposta válida, conforme critério de julgamento, para a

posterior comprovação e o exercício do direito de preferência;

b) convocação dos licitantes classificados que estejam enquadrados no inciso I do item 7.17, na ordem de classificação, para que possam oferecer nova proposta ou novo lance para igualar ou superar a melhor proposta válida, caso em que será declarado vencedor do certame;

c) caso a preferência não seja exercida na forma da alínea “b”, por qualquer motivo, serão convocadas as empresas classificadas que estejam enquadradas no inciso II do item 7.17, na ordem de classificação, para a comprovação e o exercício do direito de preferência, aplicando-se a mesma regra para o inciso III do item 7.17, caso esse direito não seja exercido.

7.19. Para o exercício do direito de preferência tratado no item 7.17, os fornecedores dos bens e serviços de informática e automação deverão declarar, no momento da apresentação da proposta, ou mediante convocação do Pregoeiro, na sessão pública, sob as penas da lei, que atendem aos requisitos estabelecidos nos incisos I, II e III do art. 5º do Decreto nº 7.174/2010, bem como, aos requisitos legais para a qualificação como microempresa ou empresa de pequeno porte, se for o caso.

7.19.1. Não estando disponível a função no sistema, o Pregoeiro fará a convocação para o critério do desempate, manualmente, via chat.

7.20. A comprovação do atendimento ao PPB ou aos bens e serviços com tecnologia desenvolvida no País será feita mediante apresentação do documento comprobatório da habilitação à fruição dos incentivos fiscais regulamentados pelo Decreto n. 5.906, de 26 de setembro de 2006, ou pelo Decreto n. 6.008, de 29 de dezembro de 2006 e será feita:

a) por meio de consulta ao sítio eletrônico oficial do Ministério da Ciência e Tecnologia ou da Superintendência da Zona Franca de Manaus - SUFRAMA; ou

b) por documento expedido para esta finalidade pelo Ministério da Ciência e Tecnologia ou pela SUFRAMA ou por outro órgão ao qual seja legalmente atribuída tal competência, mediante solicitação da licitante.

7.20.1. Não serão aceitos como meio de comprovação documentos e/ou declarações emitidas pela própria licitante ou pelo fabricante.

7.21. As microempresas e empresas de pequeno porte que atendam ao disposto nos incisos I, II e III do item 7.17 terão prioridade no exercício do direito de preferência em relação às médias e grandes empresas enquadradas no mesmo inciso.

7.22. Consideram-se bens e serviços de informática e automação com tecnologia desenvolvida no País aqueles cujo efetivo desenvolvimento local seja comprovado junto ao Ministério da Ciência e Tecnologia, na forma por este regulamentada.

8 - DA DESCONEXÃO DO(A) PREGOEIRO(A)

8.1. Na hipótese de o sistema eletrônico desconectar para o Pregoeiro no decorrer da etapa de envio de lances da sessão pública e permanecer acessível às licitantes, os lances continuarão sendo recebidos, sem prejuízo dos atos realizados.

8.2. Quando a desconexão do sistema eletrônico para o Pregoeiro persistir por tempo superior a 10 minutos, a sessão pública será suspensa e reiniciada somente decorridas 24 horas após a comunicação, no sítio <https://www.gov.br/compras/pt-br>, do fato aos participantes.

9 - DA NEGOCIAÇÃO

9.1. Encerrada a etapa de envio de lances da sessão pública, o Pregoeiro deverá encaminhar, pelo sistema eletrônico, contraproposta à licitante que tenha ofertado o melhor preço, para que seja obtida melhor proposta, vedada a negociação em condições diferentes das previstas neste Edital.

9.2. A negociação deverá ser realizada obrigatoriamente por meio do sistema, podendo ser acompanhada pelas demais licitantes.

9.3. O pregoeiro solicitará ao licitante melhor classificado que, no prazo indicado no Item 12.1, envie a proposta adequada ao último lance ofertado após a negociação realizada, acompanhada, se for o caso, dos documentos complementares, quando necessários à confirmação daqueles exigidos neste Edital e já apresentados.

10 - DA ACEITABILIDADE DA PROPOSTA

10.1. Encerrada a etapa de negociação, o(a) pregoeiro(a) examinará a proposta classificada em primeiro lugar quanto à compatibilidade do preço em relação ao máximo estipulado para a contratação e quanto à conformidade com a especificação técnica do objeto, observando-se o seguinte:

a) Não será considerada qualquer oferta de vantagem não prevista nesta licitação;

- b) Não serão aceitas propostas com valor superior ao preço máximo fixado;
- c) Não serão aceitas propostas que apresentarem preços irrisórios, de valor zero ou incompatíveis com os de mercado, exceto quando se referirem a materiais e instalações de propriedade da licitante, para os quais ela renuncie à parcela ou à totalidade da remuneração, e desde que não contrariem instrumentos legais;
- d) Não serão aceitas propostas com preços manifestamente inexequíveis, considerando como tal aqueles que, comprovadamente, forem insuficientes para a cobertura dos custos decorrentes da contratação pretendida (**Acórdão nº 1455/2018 -TCU - Plenário**).
- e) Nos preços propostos deverão estar inclusos todas as despesas para seu fornecimento, como: transportes, tributos, etc;
- f) As propostas deverão conter, obrigatoriamente, as características técnicas, **com indicação** dos part number(s) referente(s) (PartNumbers/SKUs) a cada software(s) fornecido(s), licenças de uso e garantia do produto. Adicionalmente, **a licitante deverá indicar, ponto a ponto, qual seção da documentação técnica comprova o atendimento de cada requisito e conformidade do material proposto** com a especificação exigida no termo de referência, de modo a possibilitar a análise de conformidade do material proposto com a especificação exigida, evitando a pura transcrição do disposto no Termo de Referência;
- f) A LICITANTE deverá indicar em sua proposta os fabricantes, modelos e versões de todos os componentes das soluções, incluindo componentes de hardware (se houver) e de software, realizando a indicação de todos os Códigos de Produto. Devem ser entregues prospectos/folders/folhetos com as características técnicas dos equipamentos, softwares e licenças. Devem ser apresentadas, de forma clara e detalhada, as descrições das soluções com todos os seus componentes (hardware e software), podendo ser complementadas por documentações integrantes da proposta, tais como: brochuras, catálogos, manuais técnicos, manuais de operação, etc. Na especificação técnica devem ser destacados e referenciados pelo licitante os requisitos mínimos exigidos no Termo de Referência, com a indicação do documento e página onde se encontra grifada a comprovação, sob pena de desclassificação;
- g) A LICITANTE garantirá que o bem, quer seja de sua fabricação ou integralmente ou parcialmente de subfornecedores, estará exatamente de acordo com estas especificações, isentos de defeitos de fabricação, de matéria prima ou mão de obra. Deverá, também, ser informado o prazo de garantia, conforme especificado no Termo de Referência.

10.2. O (A) Pregoeiro(a) poderá solicitar parecer de técnicos pertencentes ao quadro de pessoal do TRE/PA ou, ainda, de pessoas físicas ou jurídicas estranhas a ele, para orientar sua decisão.

10.3. Havendo aceitação da proposta classificada em primeiro lugar quanto à compatibilidade do preço, o(a) pregoeiro(a) irá avaliar as condições de habilitação da licitante.

10.4. Se a proposta não for aceitável ou se a licitante vencedora deixar de encaminhar, através de mensagem eletrônica, as especificações detalhadas do objeto, conforme solicitação constante do item 12.1, ou ainda, não atender às exigências habilitatórias, o(a) Pregoeiro(a) examinará a subsequente e, assim, sucessivamente, na ordem de classificação, até a apuração daquela que atenda aos requisitos deste Edital.

10.5. As propostas deverão possuir validade mínima de 60 (sessenta) dias.

11 - DOS DOCUMENTOS DE HABILITAÇÃO

11.1. Previamente ao exame das condições de habilitação, o Pregoeiro verificará se a licitante detentora da melhor proposta preenche as condições de participação descritas no item 2.5 deste Edital, promovendo a exclusão do certame daquela que incorra em alguma das vedações previstas.

11.1.1. Para efeito da verificação da existência de penalidade aplicada à licitante, conforme itens 2.5, “d”, “e” e “f” deste Edital, o Pregoeiro promoverá consulta ao Sistema de Cadastramento Unificado de Fornecedores (SICAF) e ao Sistema de Consulta Consolidada de Pessoa Jurídica disponibilizada pelo Tribunal de Contas da União (TCU) em <https://certidoes-apf.apps.tcu.gov.br>.

11.1.1.1. A consulta consolidada de pessoa jurídica disponibilizada pelo TCU visa atender aos princípios de simplificação e racionalização de serviços públicos digitais, tendo como fundamento legal as leis nº 12.965/2014, nº 13.460/2017 e nº 13.726/2018 e o Decreto nº 8.638/2016, reunindo informações referentes ao Sistema Inabilitados e Inidôneos do Tribunal de Contas da União (<https://contas.tcu.gov.br/ords/f?p=INABILITADO:CERTIDAO>), ao Cadastro Nacional de Condenações Cíveis por Ato de Improbidade Administrativa (www.cnj.jus.br) e aos Cadastros Nacionais de Empresas Inidôneas e Suspensas e de Empresas Punidas mantidos pela Controladoria-Geral da União - CGU (www.portaltransparencia.gov.br).

11.1.1.2. Para efeito da verificação de eventual participação indireta que ofenda ao art. 9º, III, da Lei nº 8.666/93, conforme item 2.5, “g” deste Edital, o Pregoeiro promoverá consulta ao Sistema de Cadastramento Unificado de Fornecedores (SICAF), a fim de verificar a composição societária das empresas.

11.1.2.1. Caso conste na Consulta de Situação do Fornecedor a existência de Ocorrências Impeditivas Indiretas, o pregoeiro diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas.

11.1.2.2. A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros.

11.1.2.3. O licitante será convocado para manifestação previamente à sua desclassificação/inabilitação.

11.1.3. As consultas previstas nos subitens anteriores realizar-se-ão em nome da empresa licitante, bem como de eventual matriz ou filial e de seu sócio majoritário, por força do disposto no art. 12 da Lei nº 8.429/92.

11.2. Efetuada a verificação referente ao cumprimento das condições de participação, a habilitação das licitantes será analisada pelo Pregoeiro, por meio do SICAF e da documentação complementar especificada neste Edital.

11.3. Na habilitação serão avaliados, por meio do SICAF, os seguintes documentos:

a) registro comercial, no caso de empresário pessoa física;

b) ato constitutivo, devidamente inscrito, no caso de sociedades simples, acompanhado da documentação de eleição de seus administradores e da prova de constituição da diretoria em exercício, e, no caso de sociedades empresárias, estatuto ou contrato social e alterações, devidamente registrados na Junta Comercial;

c) número da inscrição no Cadastro Nacional de Pessoa Jurídica - CNPJ do Ministério da Fazenda;

d) prova de regularidade com a Fazenda Nacional e com a Dívida Ativa da União, a ser feita pela apresentação de Certidão Conjunta emitida pela Receita Federal do Brasil e Procuradoria Geral da Fazenda Nacional, nos termos do Decreto 6.106 de 30 de abril de 2007, abrangendo, inclusive, as contribuições sociais previstas nas alíneas 'a' a 'd' do parágrafo único do art. 11 da Lei no 8.212, de 24 de julho de 1991.

e) prova de regularidade com a Fazenda Estadual (Certidão Negativa de Natureza Tributária, ou outra equivalente, na forma da Lei);

f) prova de regularidade com a Fazenda Municipal (Certidão Negativa de Natureza Tributária, ou outra equivalente, na forma da Lei);

g) prova de regularidade para com o Fundo de Garantia do Tempo de Serviço – FGTS através da apresentação do Certificado de Regularidade do FGTS - CRF;

h) prova de regularidade perante a Justiça do Trabalho, em substituição à consulta ao sítio do Tribunal Superior do Trabalho (www.tst.jus.br) referente à Certidão Negativa de Débitos Trabalhistas (CNDT), por meio da qual se comprova a inexistência de débitos inadimplidos perante a Justiça do Trabalho, ou Certidão Positiva com efeitos de negativa, quando verificada a existência de débitos garantidos por penhora suficiente ou com exigibilidade suspensa, nos termos da Lei nº 12.440/2011.

i) a certidão negativa de falência expedida pelo distribuidor da sede da pessoa jurídica, em Consulta – Cadastro - Nível VI - Qualificação Econômico-Financeira, devendo ser verificado o registro dos dados referentes à Certificação de Falência / Recuperação, (Código de Controle da Certidão, Data da Emissão e Data de Validade).

i.1) Na ausência dessa informação no SICAF, a licitante deverá apresentar a Certidão Negativa de feitos de falência, recuperação judicial ou recuperação extrajudicial expedida pelo Cartório Distribuidor da sede da licitante, dentro do prazo de validade previsto na própria certidão ou, na omissão desta, expedida a menos de 180 (cento e oitenta) dias contados da data de sua apresentação, exceto quando a pessoa jurídica não se sujeitar à falência, como no caso das cooperativas, conforme art. 4º da Lei Federal nº 5.764, de 6 de dezembro de 1971.

11.3.1. Será aceito o Certificado da matriz em substituição ao da filial, ou vice-versa, quando comprovadamente houver arrecadação centralizada.

11.3.2. Caso não exista, no SICAF, o registro da documentação exigida no Item 11.3, ou se, nos registros cadastrais existentes, constar algum documento vencido, a licitante deverá encaminhar comprovante equivalente, com o respectivo prazo atualizado, conforme estipulado no art. 26 do Decreto nº 10.024/2019, sob pena de inabilitação.

11.3.3 O(a) Pregoeiro(a), no momento da habilitação da licitante que ofertou o melhor lance, deverá consultar sítios oficiais de órgãos e entidades emissores de certidões para verificar se as condições de habilitação relativas às regularidades fiscal e trabalhista estão mantidas.

11.3.3.1 Se, com a consulta acima mencionada, o(a) pregoeiro(a) constatar alguma restrição na comprovação das regularidades fiscal e trabalhista da licitante, deverá, a depender do caso concreto, inabilitá-la ou proceder na forma do Item 11.3.4 deste Edital.

11.3.4. Em se tratando de microempresa, empresa de pequeno porte ou sociedade cooperativa que tenha auferido, no ano-calendário anterior, receita bruta até o limite definido no inciso II do caput do art. 3º da Lei Complementar no 123/06 e alterações e art. 34 da Lei 11.488/07, havendo alguma restrição na regularidade fiscal e trabalhista, será assegurado o prazo de 5 (cinco) dias úteis, prorrogáveis por igual período, a critério da Administração, para regularização da documentação, pagamento ou parcelamento do débito e emissão de eventuais certidões negativas ou positivas com efeito de negativa.

11.3.4.1. O prazo para regularização fiscal e trabalhista previsto no item 11.3.4 será contado a partir da divulgação do resultado da fase de habilitação.

11.3.4.2. A prorrogação do prazo previsto no item 11.3.4 poderá ser concedida, a critério da administração pública, quando requerida pela licitante, mediante apresentação de justificativa.

11.3.4.3. A abertura da fase recursal em relação ao resultado do certame ocorrerá após os prazos de regularização fiscal de que tratam os itens 11.3.4.1 e 11.3.4.2.

11.3.5. A não regularização da documentação implicará decadência do direito à assinatura do contrato / Ata de Registro de Preços, sem prejuízo das sanções previstas no art. 7º da Lei nº 10.520/2002, sendo facultado à Administração convocar as licitantes remanescentes, na ordem de classificação, para assinatura do contrato / da Ata, ou revogar a licitação.

11.3.6. As licitantes poderão deixar de apresentar os documentos de habilitação que constem no SICAF, assegurados aos demais o direito de acesso aos dados constantes dos sistemas.

11.3.6.1. Ao Pregoeiro incumbe emitir, no dia em que iniciar a análise da documentação habilitatória, espelho do SICAF, de modo a aferir a habilitação da licitante, nos documentos por ele abrangidos, nos termos do item 11.3.

11.3.6.2. É dever da licitante atualizar previamente as comprovações constantes do SICAF para que estejam vigentes na data da abertura da sessão pública, ou encaminhar, em conjunto com a apresentação da proposta, a respectiva documentação atualizada.

11.3.6.3. O descumprimento do subitem acima implicará a inabilitação do licitante, exceto se a consulta aos sítios eletrônicos oficiais emissores de certidões feita pelo Pregoeiro lograr êxito em encontrar a(s) certidão(ões) válida(s), conforme art. 43, §3º, do Decreto 10.024, de 2019.

11.3.6.4. Nos termos do subitem 12.1, “b”, caso ocorra o vencimento das certidões e demais documentos constantes do SICAF após a data da abertura da sessão pública, e a consulta aos sítios eletrônicos oficiais emissores de certidões feita pelo Pregoeiro não lograr êxito em encontrar a(s) certidão(ões) ou documento(s) válido(s), será facultado à licitante o envio dos documentos pertinentes, no prazo definido no item 12.1 deste Edital.

11.4. Para fins de habilitação, a licitante deverá apresentar, ainda, até a data e hora marcadas para a abertura da sessão, exclusivamente por meio eletrônico, **atestado(s) ou declaração (ões), fornecido (s) por pessoa jurídica de direito público ou privado**, que comprove o fornecimento e implantação de, pelo menos, 01 (um) appliance virtual e/ou físico da solução Web Application Firewall (WAF), a fim de comprovar a aptidão para desempenho de atividade pertinente e compatível com o objeto da licitação.

11.4.1. O(s) atestado(s) deverá(ão) conter as seguintes informações mínimas: nome e cargo da pessoa que os assina, quantitativo associado ao fornecimento, valor e/ou Contrato(s) associado(s) à prestação dos serviços;

11.4.2. Visando esclarecer ou complementar a instrução do processo, nos termos do §3º do art. 43 da Lei nº 8.666/1993, é facultado ao pregoeiro solicitar a licitante a disponibilização de documentos e informações adicionais necessárias à comprovação da legitimidade do(s) atestado(s) ou declaração(ões) apresentado(s), inclusive cópia de pelo menos uma nota fiscal do serviço constante no documento apresentado.

11.4.3. Ainda, em termos de diligência, o TRE-PA se reserva ao direito de entrar em contato com os gestores do contrato, realizar visita(s) ou reuniões com as entidades emissoras de forma a sanar dúvidas e atestar a veracidade das informações apresentadas. Devido a tal, todas as informações necessárias à comprovação da legitimidade dos atestados solicitados poderão ser solicitadas para averiguação. Quais sejam: cópia do contrato que deu suporte à contratação, Relatórios Técnicos de Controle ou Execução do Contrato, Notas Fiscais, Ordens de Serviço, endereço e telefones dos gestores do contrato e local em que foram prestados os serviços.

12 - DO ENCAMINHAMENTO DE INFORMAÇÕES E DOCUMENTAÇÃO PELA LICITANTE VENCEDORA

12.1. A licitante vencedora do LOTE deverá encaminhar, por meio da opção “Enviar Anexo” do Sistema Compras Governamentais, no prazo de 02 (duas) horas, contado da solicitação do(a) Pregoeiro(a), no Sistema Eletrônico:

a) Proposta contemplando preço adequado ao último lance, além de especificações detalhadas do(s) material(is), **inclusive com indicação da part number(s) referente(s) (PartNumbers/SKUs)** a cada software(s) fornecido(s), licenças de uso e garantia do produto, conforme o Anexo I do Edital - Termo de Referência, bem como número de telefone(s), e-mail, endereço, além da indicação de Banco, Agência e número da Conta Corrente;

b) Documentação complementar à proposta e à habilitação já constantes do Sistema de Compras do Governo Federal, quando necessário para confirmar informações contidas na proposta ou na documentação habilitatória, nos termos deste Edital.

12.2. Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante apresentação dos documentos originais não-digitais quando houver dúvida em relação à integridade do documento digital. Neste caso, o Pregoeiro fará a solicitação pelo *chat* da sessão pública virtual e indicará o endereço para envio da documentação solicitada.

12.3. O número de inscrição no CNPJ da empresa deverá ser o mesmo da documentação apresentada para habilitação, da Proposta Comercial e do documento de cobrança, servindo de base para emissão da Nota de Empenho.

12.3.1. Na hipótese de o documento de cobrança estar em nome da filial, esta deverá comprovar sua regularidade estadual, conforme o caso.

12.3.2. Se o licitante for a matriz, todos os documentos deverão estar em nome da matriz, e se o licitante for a filial, todos os documentos deverão estar em nome da filial, exceto aqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.

13 - DOS RECURSOS

13.1. Declarado o vencedor, o Pregoeiro abrirá o prazo de 30 (trinta) minutos, durante o qual qualquer licitante poderá, de forma imediata e motivada, em campo próprio do sistema, manifestar sua intenção de recorrer, registrando a síntese de suas razões.

13.1.1. O Pregoeiro examinará a intenção de recurso, aceitando-a ou, motivadamente, rejeitando-a, em campo próprio do sistema.

13.1.2. A recorrente que tiver sua intenção de recurso aceita deverá registrar as razões do recurso, em campo próprio do sistema, no prazo de 03 (três) dias, ficando as demais licitantes, desde logo, intimadas a apresentar contrarrazões, também via sistema, em igual prazo, que começará a correr do término do prazo da recorrente.

13.2. Os autos do processo permanecerão com vista franqueada aos interessados.

13.3. A falta de manifestação imediata e motivada da intenção da licitante em recorrer importará na decadência do direito ao recurso e o Pregoeiro adjudicará, POR LOTE, o objeto do certame à(s) empresa(s) declarada(s) vencedora(s), sendo submetido o presente procedimento ao (à) Diretor(a) Geral para homologação.

13.4. O(s) recurso(s), porventura interposto(s), não terá(ão) efeito suspensivo e será(ão) dirigido(s) ao(a) Diretor(a) Geral do TRE/PA, por intermédio do(a) Pregoeiro(a), o(a) qual poderá reconsiderar sua decisão, em 05 (cinco) dias úteis ou, nesse mesmo período, encaminhá-lo(s) ao(a) Diretor(a) Geral do TRE/PA, devidamente informado(s), para apreciação e decisão, no mesmo prazo, contado do recebimento do recurso, sob pena de responsabilidade.

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

13.6. Decidido(s) o(s) recurso(s), o (a) Diretor (a) Geral do TRE/PA fará a adjudicação do objeto à licitante vencedora, POR LOTE, e homologará o procedimento licitatório.

14 - DA IMPUGNAÇÃO DO ATO CONVOCATÓRIO E DO PEDIDO DE ESCLARECIMENTO

14.1. Até 3 dias úteis anteriores à data fixada para abertura da sessão pública, qualquer pessoa poderá impugnar o presente ato convocatório, exclusivamente por meio eletrônico, via internet, nos seguintes endereços: pregoeiros@tre-pa.jus.br, coinf@tre-pa.jus.br e selic@tre-pa.jus.br.

14.2. Caberá ao Pregoeiro(a), auxiliado pelo setor responsável pela elaboração do Edital, decidir sobre a impugnação, no prazo de dois dias úteis, contados da data de recebimento da Impugnação.

14.2.1. A impugnação não possui efeito suspensivo. A concessão de efeito suspensivo é medida excepcional, devendo ser motivada pelo Pregoeiro, nos autos do Processo de licitação.

14.3. Acolhida a petição contra o ato convocatório, será designada nova data para realização do certame.

14.4. Os pedidos de esclarecimento referentes ao presente Edital serão enviados ao Pregoeiro, até 03 dias úteis anteriores à data fixada para abertura da sessão pública, exclusivamente por meio eletrônico via internet, nos seguintes endereços: pregoeiros@tre-pa.jus.br, coinf@tre-pa.jus.br e selic@tre-pa.jus.br.

14.5. O Pregoeiro responderá aos pedidos de esclarecimento no prazo de 2 dias úteis, contados da data de recebimento do pedido, podendo requisitar subsídios formais aos responsáveis pela elaboração do Edital.

14.5.1. As respostas aos pedidos de esclarecimento vincularão os participantes e a Administração.

14.6. Os pedidos de esclarecimento e as impugnações serão divulgados no sítio eletrônico <https://www.gov.br/compras/pt-br> (por meio do link Acesso livre – Pregões – Agendados).

15 - DO CRITÉRIO DE JULGAMENTO DAS PROPOSTAS

15.1 No julgamento das propostas será adotado o critério do **MENOR PREÇO GLOBAL POR LOTE**, observadas as exigências estabelecidas neste Edital e seus Anexos.

15.1.1. Considerar-se-á menor preço global do lote (Letra “D” da tabela constante do Item 4.7 do Anexo I – Termo de Referência), o valor correspondente à soma do valor global dos itens que compõem o lote.

15.1.2. O valor global de cada item (Letra "C" da tabela constante do Item 4.7 do Anexo I – Termo de Referência) será obtido mediante a multiplicação da quantidade registrada ("A" da tabela constante do Item 4.7 do Anexo I – Termo de Referência) com o valor unitário registrado para cada unidade ("B" da tabela constante do Item 4.7 do Anexo I – Termo de Referência)."

15.2. O valor máximo para fins de aceitabilidade da proposta dos respectivos lotes, bem como dos itens que os compõem, encontra-se na planilha constante do item 4.7 do Termo de Referência, não podendo ser aceitas pelo pregoeiro(a) propostas com valores acima dos previstos pela Administração;

15.3. Caso a licitante vencedora apresente sua proposta com valores unitários superiores aos fixados, deverá o(a) pregoeiro(a), em diligência, solicitar o ajuste da proposta aos valores máximos permitidos, sendo que o não atendimento da diligência no prazo fixado ou a recusa em fazê-lo caracterizará hipótese de desclassificação da proposta.

15.4. O Pregoeiro poderá, no julgamento da habilitação e das propostas, sanar erros ou falhas que não alterem a substância das propostas, dos documentos e sua validade jurídica, mediante decisão fundamentada, registrada em Ata e acessível aos licitantes, e lhes atribuirá validade e eficácia para fins de habilitação e classificação.

15.4.1. Na hipótese de necessidade de suspensão da sessão pública para realização de diligências, visando ao saneamento dos erros ou falhas de que trata o item 15.4, a sessão pública somente poderá ser reiniciada mediante aviso prévio no sistema com, no mínimo, 24 horas de antecedência, tudo registrado em Ata.

16 - DA DESPESA E DOS RECURSOS ORÇAMENTÁRIOS

16.1. A despesa com a execução do objeto desta licitação é estimada em **R\$ 40.049.395,26 (quarenta milhões, quarenta e nove mil, trezentos e noventa e cinco reais e vinte e seis centavos)**, conforme planilhas constantes do Anexo I.

16.2. A despesa decorrente da presente licitação correrá à conta de recursos previstos no Orçamento da Justiça Eleitoral, na Ação 20GP.0015 – Julgamento de Causas e Gestão Administrativa na Justiça Eleitoral.

17 – DA ATA DE REGISTRO DE PREÇOS

17.1. A Administração do TRE/PA convocará a(s) licitante(s) vencedora(s), por escrito, para assinar a Ata de Registro de Preços, no prazo máximo de 05 (cinco) dias úteis, contados do recebimento da convocação, podendo ser prorrogado uma vez, por igual período, quando solicitado pela adjudicatária, desde que ocorra motivo justificado aceito pela Administração.

17.2. A Ata de Registro de Preços, documento vinculativo, obrigacional, que representa o compromisso a ser firmado entre o TRE/PA e a(s) licitante(s) vencedora(s) do certame, será formalizada de acordo com o **Anexo correspondente do Edital** e terá validade de 12 (doze) meses, contados da data de sua assinatura.

17.2.1. A convocação para a assinatura da Ata de Registro de Preços dar-se-á por meio do Sistema Eletrônico de Informação – SEI deste Tribunal.

17.2.2. Para poder efetivar a assinatura eletrônica da Ata de Registro de Preços, a licitante vencedora deverá estar cadastrada no Sistema Eletrônico de Informação deste Tribunal.

17.2.3. Caso não possua o referido cadastro, será enviado link de página da internet, para o e-mail do responsável pela assinatura da Ata de Registro de Preços, como forma de se implementar a assinatura eletrônica.

17.2.4. Excepcionalmente, poderá ser autorizada a assinatura da Ata de Registro de Preços em instrumento físico, lavrado em duas vias de igual teor e forma.

17.3. O Sistema de Registro de Preços não obriga a compra / contratação de serviços, nem mesmo nas quantidades indicadas no Anexo I deste edital, podendo a Administração promover a aquisição em unidades de acordo com suas necessidades.

17.4. O Tribunal Regional Eleitoral do Pará não está obrigado, durante o prazo de validade do Registro de Preços decorrente deste certame, a firmar as contratações que dele poderão advir, podendo realizar licitações específicas para a aquisição pretendida, ficando assegurado ao beneficiário do registro a preferência de fornecimento em igualdade de condições.

17.5. O direito de preferência de que trata o subitem anterior poderá ser exercido pelo beneficiário do registro quando o Tribunal Regional Eleitoral do Pará, após realizada a licitação específica, constatar que o preço obtido é igual ou maior que o registrado ou, após negociação, aquiescer o detentor da ata em baixar o preço registrado, igualando ou tornando-o menor que o obtido em referida licitação.

17.6. Se a(s) licitante(s) vencedora(s) não comprovar(em) a manutenção das condições de habilitação consignadas no Edital ou recusar(em)-se a assinar a Ata de Registro de Preços, sem justificativa por escrito, aceita pelo(a) Diretor(a)-Geral, será(ão) convocada(s) a(s) licitante(s) constante(s) no cadastro reserva a que se refere o item 17.13 para assinatura da Ata de Registro de Preços, desde que cumpridos os requisitos de habilitação, sem prejuízo da aplicação das sanções administrativas previstas no item 19.1 deste Edital e art. 81 da Lei nº 8.666/93.

17.6.1. Não havendo cadastro de reserva, o Pregoeiro(a) retornará à fase de aceitação das propostas e examinará as ofertas subsequentes e a qualificação dos licitantes, respeitada a ordem de classificação, para, após comprovados os requisitos habilitatórios e feita a negociação, declarar a respectiva licitante vencedora, celebrando com ela o compromisso representado pela assinatura da Ata de Registro de Preços.

17.7. Os preços ofertados e registrados não poderão ser majorados, porém poderão ser revistos em decorrência de eventual redução daqueles praticados no mercado, ou de fato que eleve o custo dos serviços ou bens registrados, cabendo ao TRE-PA promover as necessárias negociações junto aos fornecedores, observadas as disposições contidas na alínea “d” do inciso II do caput do art. 65 da Lei n.º 8.666/1993.

17.8. A Ata de Registro de Preços poderá ser utilizada pelos Tribunais Regionais Eleitorais que não tenha participado do certame licitatório, mediante prévia consulta e anuência deste TRE-PA, na qualidade de órgão gerenciador da Ata, observadas, ainda, as demais regras impostas no art. 22 do Decreto n.º 7.892/2013.

17.8.1. O fornecedor beneficiário da ata de registro de preços poderá optar pela aceitação ou não da prestação do serviço decorrente de adesão, desde que não prejudique as obrigações presentes e futuras decorrentes da ata, assumidas perante o TRE-PA.

17.8.2. O órgão ou entidade interessado em utilizar a ata formalizada por este Tribunal deverá apresentar estudo demonstrando o ganho de eficiência, a viabilidade e a economicidade decorrentes do procedimento.

17.8.3. As aquisições ou contratações adicionais a que se refere este item não poderão exceder, por órgão ou entidade, a cinquenta por cento dos quantitativos registrados.

17.8.4. O quantitativo decorrente das adesões à ata de registro de preços não poderá exceder, na totalidade, ao dobro dos quantitativos registrados, independentemente do número de órgãos não participantes que aderirem.

17.8.5. Após a autorização do TRE-PA, o órgão não participante deverá efetivar a aquisição ou contratação solicitada em até noventa dias, observado o prazo de vigência da ata.

17.8.6. Nas licitações processadas por meio do Sistema de Registro de Preços, destinadas à contratação exclusiva de Microempresas e Empresas de Pequeno Porte, o somatório das contratações, na totalidade, incluindo as realizadas por este Tribunal, não excederão o valor de R\$ 80.000,00 para cada item registrado, conforme Acórdão TCU nº 1.968/2015 – Plenário.

17.9. As obrigações do órgão gerenciador e dos órgãos participantes da ata são as seguintes:

17.9.1. São obrigações do órgão gerenciador da ata:

17.9.1.1. Gerenciar a Ata de Registro de Preços, indicando, sempre que solicitado, o nome do detentor da ata, o preço, e as especificações dos materiais registrados, observada a ordem de classificação indicada na licitação.

17.9.1.2. Observar para que, durante a vigência da ata, sejam mantidas todas as condições de habilitação e qualificação exigidas na licitação, bem assim, a compatibilidade com as obrigações assumidas.

17.9.1.3. Conduzir eventuais procedimentos administrativos de renegociação de preços registrados, para fins de adequação às novas condições de mercado, e de aplicação de penalidades.

17.9.1.4. Acompanhar a evolução dos preços de mercado, com a finalidade de verificar sua compatibilidade com aqueles registrados na ata.

17.9.1.5. Acompanhar e fiscalizar o cumprimento das condições ajustadas na Ata.

17.9.1.6. Consultar o detentor da ata registrada (observada a ordem de classificação) quanto ao interesse em fornecer os bens a outro(s) órgão da Administração Pública que externe(m) a intenção de utilizar a presente Ata, conforme item 17.8

17.9.1.7. Gerenciar seus próprios pedidos decorrentes do Registro de Preços;

17.9.1.8. Aplicar, garantida a ampla defesa e o contraditório, as penalidades decorrentes do descumprimento do pactuado na ata de registro de preços ou do descumprimento das obrigações contratuais, em relação às suas próprias contratações.

17.9.2. São obrigações do órgão participante:

17.9.2.1. Tomar conhecimento da ata de registros de preços, inclusive de eventuais alterações, para o correto cumprimento de suas disposições;

17.9.2.2. Gerenciar seus próprios pedidos decorrentes do Registro de Preços;

17.9.2.3. Aplicar, garantida a ampla defesa e o contraditório, as penalidades decorrentes do descumprimento do pactuado na ata de registro de preços ou do descumprimento das obrigações contratuais, em relação às suas próprias contratações.

17.9.2.4. Por ocasião da celebração dos contratos, observar os quantitativos registrados para cada órgão.

17.10. São obrigações do detentor da ata:

17.10.1. Assinar o contrato, no prazo de 05 (cinco) dias úteis, a contar da data do recebimento da convocação, podendo tal prazo ser prorrogado uma vez, por igual período, quando solicitado pela adjudicatária, desde que ocorra motivo justificado aceito pela Administração, estando as obrigações assumidas vinculadas à proposta, aos lances, ao edital e à respectiva Ata.

17.10.2 Fornecer os bens obedecendo rigorosamente ao disposto no anexo I (Termo de Referência) deste Edital.

17.10.3. Providenciar a imediata correção de deficiências, falhas ou irregularidades constatadas pelo ÓRGÃO GERENCIADOR, referentes às condições firmadas na Ata.

17.10.4. Viabilizar o atendimento das condições firmadas a partir da data da assinatura da Ata.

17.10.5. Manter durante o prazo de vigência da Ata, todas as condições de habilitação exigidas neste Edital.

17.10.6. Informar no prazo máximo de 05 (cinco) dias úteis, contados do recebimento da notificação, quanto à aceitação ou não da prestação do serviço a outro órgão da Administração Pública (não participante) que venha a manifestar o interesse de utilizar a presente Ata, conforme item 17.8.

17.11. A ata de registro de preços poderá sofrer alterações, observadas as seguintes disposições:

17.11.1. O gerenciador da Ata de Registro de Preços acompanhará a evolução dos preços de mercado, com a finalidade de verificar sua compatibilidade com aqueles registrados na ata.

17.11.2. Serão considerados compatíveis com os de mercado os preços registrados que forem iguais ou inferiores a média daqueles apurados pelo Tribunal Regional Eleitoral do Pará, por intermédio do órgão gerenciador do registro de preços.

17.11.3. Quando o preço inicialmente registrado tornar-se superior ao preço médio praticado no mercado, o órgão gerenciador solicitará ao detentor da ata, por escrito, redução do preço registrado, de forma a adequá-lo aos níveis definidos nos termos do subitem anterior.

17.11.4. Caso o detentor da ata não concorde em reduzir o preço, será liberado do compromisso assumido, devendo o órgão gerenciador convocar os demais licitantes, visando igual oportunidade de negociação.

17.11.5. Quando o preço de mercado tornar-se superior aos preços registrados e o detentor da ata, mediante requerimento devidamente comprovado, não puder cumprir o compromisso, o órgão gerenciador poderá:

a) liberar o detentor da ata do compromisso assumido, sem aplicação da penalidade, confirmando a veracidade dos motivos e comprovantes apresentados, e se a comunicação ocorrer antes do pedido de fornecimento;

b) convocar os demais detentores da ata visando igual oportunidade de negociação.

17.11.6. Não havendo êxito nas negociações de que tratam os subitens anteriores, o órgão gerenciador deverá proceder à revogação da Ata de Registro de Preços.

17.11.7. O(s) contrato(s) advindo(s) da Ata poderá(ão) sofrer alterações, obedecidas às disposições contidas no art. 65, da Lei 8.666/93.

17.12. O detentor da ata, assegurados o contraditório e a ampla defesa, poderá ter seu registro cancelado:

17.12.1. A pedido, quando:

a) Comprovar estar impossibilitado de cumprir as exigências da ata, por ocorrência de caso fortuito ou de força maior;

b) O preço registrado se tornar, comprovadamente, inexecúvel em função da elevação dos preços de mercado, dos insumos que compõem o custo das aquisições/contratações, desde que a comunicação ocorra antes do pedido de fornecimento.

17.12.2. Por iniciativa do TRE/PA, quando:

a) O detentor da ata não aceitar reduzir o preço registrado, na hipótese deste se tornar superior àqueles praticados no mercado;

b) O detentor da ata perder qualquer condição de habilitação exigida no processo licitatório;

c) Por razões de interesse público, quando devidamente motivadas e justificadas;

d) O detentor da ata deixar de cumprir as obrigações dela decorrentes;

e) O detentor da ata não comparecer ou se recusar a assinar o contrato, no prazo estabelecido.

f) O detentor da ata sofrer sanção prevista nos [incisos III ou IV do caput do art. 87 da Lei nº 8.666/1993](#) ou no [art. 7º da Lei nº 10.520/2002](#).

17.13. Por ocasião da homologação do certame no Sistema Compras governamentais, a Autoridade Superior concederá o prazo de 24 (vinte e quatro) horas para que as demais licitantes registrem, também no sítio eletrônico em que transcorre

o procedimento licitatório, sua intenção de cotar os bens ou serviços com preços iguais ao da licitante vencedora, na sequência da classificação do certame, excluído o percentual referente à margem de preferência, quando o objeto não atender aos requisitos previstos no art. 3º da Lei nº 8.666/93.

17.13.1. O registro a que se refere o item 17.13 tem por objetivo a formação de cadastro de reserva, conforme art. 11 do Decreto nº 7.892/13, no caso de impossibilidade de atendimento pelo primeiro colocado da ata, nas hipóteses previstas no item 17.12.

17.13.2. Se houver mais de uma licitante interessada em compor o cadastro de reserva, serão classificados segundo a ordem da última proposta apresentada durante a fase competitiva.

17.13.3. A habilitação dos fornecedores que comporão o cadastro de reserva será verificada quando houver necessidade de contratação do fornecedor remanescente.

17.13.4. O cadastro de reserva abrangerá apenas os itens com propostas adjudicadas no Sistema Comprasgovernamentais.

17.13.5. Findo o prazo para manifestação dos interessados, será gerada a competente ATA DE FORMAÇÃO DE CADASTRO RESERVA pelo sistema, que conterà a informação dos licitantes que aceitarem cotar os bens ou serviços com preços iguais ao da licitante vencedora do certame.

17.14. O Órgão Gerenciador da Ata será o TRIBUNAL REGIONAL ELEITORAL DO PARÁ, UASG 070004.

17.14.1. São participantes os seguintes Órgãos:

- a) TRIBUNAL REGIONAL ELEITORAL DO RIO DE JANEIRO - UASG 70017;
- b) TRIBUNAL REGIONAL ELEITORAL DE SÃO PAULO.- UASG 70018;
- c) TRIBUNAL REGIONAL ELEITORAL DE SERGIPE -UASG 70012;
- d) TRIBUNAL REGIONAL ELEITORAL DO PARANÁ - UASG 70019;
- e) TRIBUNAL REGIONAL ELEITORAL DE TOCANTINS - UASG 70027;
- f) TRIBUNAL REGIONAL ELEITORAL DO DISTRITO FEDERAL - UASG 70025;
- g) TRIBUNAL REGIONAL ELEITORAL DA PARAÍBA - UASG 70009;
- h) TRIBUNAL REGIONAL ELEITORAL DE PERNAMBUCO - UASG 70010;
- i) TRIBUNAL REGIONAL ELEITORAL DO AMAZONAS - UASG 70003;
- j) TRIBUNAL REGIONAL ELEITORAL DE SANTA CATARINA - UASG 70020;
- k) TRIBUNAL REGIONAL ELEITORAL DO ACRE - UASG 70002;
- l) TRIBUNAL REGIONAL ELEITORAL DO MATO GROSSO DO SUL - UASG 70016;
- m) TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE - UASG 70008;
- n) TRIBUNAL REGIONAL ELEITORAL DO CEARÁ - UASG 70007;
- o) TRIBUNAL REGIONAL ELEITORAL DO ESPÍRITO SANTO - UASG 70015;
- p) TRIBUNAL REGIONAL ELEITORAL DE RONDÔNIA - UASG 70024;
- q) TRIBUNAL REGIONAL ELEITORAL DO AMAPÁ - UASG 70029;
- r) TRIBUNAL REGIONAL ELEITORAL DE GOIÁS - UASG 70023.

17.4.2. Por ocasião da celebração dos contratos, o órgão gerenciador e os órgãos participantes deverão observar os quantitativos registrados para cada órgão.

18 - DO CONTRATO E DO PAGAMENTO

18.1 Será firmado contrato com a empresa licitante vencedora, estando as obrigações assumidas vinculadas à proposta, aos lances, ao Edital e à Lei n.º 8.666/93.

18.2. A Administração do Tribunal Regional Eleitoral do Pará convocará a adjudicatária, por escrito, para assinar o Contrato no prazo de 05 (cinco) dias úteis, contados do recebimento da convocação, podendo ser prorrogado uma vez, por igual período, quando solicitado pela adjudicatária, desde que ocorra motivo justificado aceito pela Administração.

18.2.1. A convocação para a assinatura do contrato dar-se-á por meio do Sistema Eletrônico de Informação – SEI deste Tribunal.

18.2.2. Para poder efetivar a assinatura eletrônica do contrato, a licitante vencedora deverá estar cadastrada no Sistema Eletrônico de Informação deste Tribunal.

18.2.3. Caso não possua o referido cadastro, será enviado link de página da internet, para o e-mail do responsável pela assinatura do contrato, como forma de se implementar a assinatura eletrônica.

18.2.4. Excepcionalmente, poderá ser autorizada a assinatura, pelas partes e testemunhas, de instrumento de contrato, lavrado em duas vias de igual teor e forma.

18.2.5. A convocação da adjudicatária, para assinatura do Contrato, por parte dos Órgãos Participantes, dar-se-á no prazo indicado no item 18.2, mas observará os procedimentos próprios adotados por cada órgão.

18.3. O(A) Pregoeiro(a), sem prejuízo da aplicação das sanções administrativas previstas no item 19 deste Edital e art. 81 da Lei nº 8.666/93, examinará as ofertas subsequentes e a qualificação das licitantes, respeitada a ordem de classificação para, após comprovados os requisitos habilitatórios e feita a negociação, declarar a respectiva licitante vencedora, celebrando com ela o contrato, se o vencedor da licitação:

a) por ocasião da assinatura do contrato, não comprovar a manutenção das condições de habilitação consignadas no Edital;

b) recusar-se a assinar o contrato, sem justificativa por escrito, aceita pelo(a) Diretor(a)-Geral.

18.4. O pagamento será efetuado através de Ordem Bancária, mediante depósito na conta-corrente da Contratada, até o 10º (décimo) dia útil da data da liquidação da despesa, observado o estabelecido no art. 5º da Lei nº 8.666/93, e desde que não ocorra fator impeditivo provocado pela Contratada.

18.4.1 Será considerada data do pagamento o dia em que constar como emitida a ordem bancária de pagamento.

18.4.2 No caso do valor do pagamento não ultrapassar o limite de que trata o inciso II do art. 24, da Lei nº 8.666/93, o mesmo deverá ser efetuado no prazo de até 5 (cinco) dias úteis, nas condições referidas no item 18.4.

18.4.3. Nenhum pagamento será efetuado à CONTRATADA enquanto pendente de liquidação qualquer obrigação financeira que lhe for imposta, em virtude de penalidade ou inadimplência, sem que isso gere direito ao pleito de reajustamento dos preços ou correção monetária.

18.5. Para fazer jus ao pagamento a CONTRATADA deverá apresentar Nota Fiscal/Fatura discriminando o fornecimento/serviço efetivamente prestado.

18.5.1. Se optante pelo Simples Nacional, deverá ser apresentada a declaração de que trata o art. 6º da Instrução Normativa nº 1234/2012, em meio físico ou eletrônico assinado por certificação digital (não será aceito simples cópia digitalizada).

18.6. Os pagamentos serão realizados após a comprovação da regularidade fiscal e trabalhista exigidas na habilitação, mediante a consulta “on-line” junto ao Sistema de Cadastramento Unificado de Fornecedores – SICAF.

18.6.1. Constatada a situação de irregularidade fiscal da contratada, será providenciada a sua notificação, por escrito, no sentido de que, no prazo de cinco (05) dias úteis, a contratada regularize sua situação ou, no mesmo prazo, apresente sua defesa.

18.6.2. O prazo do item anterior poderá ser prorrogado uma vez, por igual período, a critério da Administração.

18.6.3. Não havendo regularização ou sendo a defesa considerada improcedente, a Administração comunicará os órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência do fornecedor, bem como quanto à existência de pagamento a ser efetuado pela Administração, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

18.6.4. Persistindo a irregularidade, a Administração deverá adotar as medidas necessárias à rescisão do contrato, assegurada à contratada a ampla defesa.

18.6.5. Havendo a efetiva prestação de serviços ou o fornecimento dos bens, os pagamentos serão realizados normalmente, até que se decida pela rescisão contratual, caso a contratada não regularize sua situação.

18.6.6. Somente por motivo de economicidade, segurança nacional ou outro interesse público de alta relevância, devidamente justificado, em qualquer caso, pelo Diretor(a)-Geral, não será rescindido o contrato em execução com a contratada inadimplente.

18.7. Na ocasião do pagamento, serão efetuadas as seguintes retenções:

18.7.1. Tributos e contribuições federais (IR, CSLL, PIS e COFINS) previstos no artigo 64 da Lei nº 9.430, de 27.12.96, e [Instrução Normativa RFB nº 1.234](#), de 11.01.12, enquadrando os itens 1 e 3 a 6 no código 6190 (Demais serviços) e o item 2 no código 6147 (Mercadorias e bens em geral) da Tabela de Retenção do Anexo I da referida Instrução Normativa, exceto quando se tratar de empresa optante pelo simples nacional, hipótese em que deverá ser apresentada, no ato da assinatura do contrato, a declaração prevista no Anexo IV da mesma Instrução Normativa; e

18.7.2. Imposto Sobre Serviços (ISS) previsto na [Lei Complementar nº 116](#), de 31.07.03, enquadrando os licenciamentos da solução (itens 1 e 3) no item 1.05 da Lista de Serviços anexa à referida Lei, os serviços de instalação e de operação

assistida (itens 4 e 6) no item 1.07 e o treinamento (item 5) no item 8.02 da mesma Lista. Para efeito do disposto neste tópico será observado o contido nos artigos 3º e 4º da Lei Complementar nº 116/2003 (local do estabelecimento prestador). Em se tratando de empresa optante pelo simples nacional, a retenção se dará conforme enquadramento no respectivo Anexo da [Lei Complementar nº 123/2006](#).

18.8. Para efeito do disposto no item 18.7, a empresa deverá destacar no documento fiscal as alíquotas dos tributos e das contribuições, bem como os correspondentes valores, nos termos das respectivas legislações. Em caso de descumprimento desta determinação, a empresa sofrerá a retenção pelas alíquotas máximas previstas.

18.9. Na hipótese de ocorrer alteração em alguma das normas referenciadas no item 18.7, será aplicada a retenção correspondente prevista na legislação em vigor.

18.10. No caso de eventual atraso de pagamento, desde que a CONTRATADA não tenha concorrido de alguma forma para tanto, fica convencionado que a taxa de atualização financeira devida pela CONTRATANTE, entre a data acima referida e a correspondente ao efetivo adimplemento da parcela, será calculada mediante a aplicação da seguinte 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 a ser paga; e

I = Índice de atualização financeira = 0,0001644, assim apurado:

$$I = (TX/100)/365$$

$$I = (6/100)/365$$

$$I = 0,0001644$$

TX = Percentual da taxa anual = 6%

18.11. Nenhum pagamento será efetuado à Contratada enquanto pendente de liquidação qualquer obrigação financeira que lhe for imposta, em virtude de penalidade ou inadimplência, sem que isso gere direito ao pleito de reajustamento dos preços ou correção monetária.

18.12. Não serão aceitas cobranças realizadas através de títulos colocados em cobrança através de banco ou outra instituição do gênero.

18.13. As notas fiscais/faturas apresentadas em desacordo com o estabelecido neste Edital ou com qualquer vício serão devolvidas à CONTRATADA, não correndo, neste caso, o prazo estipulado no item 18.4 deste edital, iniciando-se, somente, a partir da sua completa regularização.

18.14. O reajustamento dos preços objeto do presente certame se dará nos termos previstos no instrumento de contrato, conforme minuta anexa ao presente Edital

19 - DAS SANÇÕES ADMINISTRATIVAS

19.1. Ficará impedida de licitar e de contratar com a União e será descredenciada no SICAF, pelo prazo de até cinco anos, sem prejuízo das multas previstas em edital e no contrato e das demais cominações legais, garantido o direito à ampla defesa, a licitante que, convocada dentro do prazo de validade de sua proposta:

- a) Deixar de entregar a documentação exigida no Edital;
- b) Não assinar a Ata de Registro de Preços ou o contrato e/ou não receber a Ordem de Fornecimento e/ou de Serviço;
- c) Apresentar documento falso ou fizer declaração falsa;
- d) Causar atraso na execução do objeto deste Pregão;
- e) Não manter a proposta, injustificadamente;
- f) Falhar ou fraudar na execução do contrato;
- g) Comportar-se de modo inidôneo;
- h) Cometer fraude fiscal.

19.2. Sem prejuízo das demais sanções previstas no art. 87 da Lei nº 8.666/93, pelo atraso injustificado e inexecução total ou parcial do objeto deste Pregão, a Administração do Tribunal Regional Eleitoral do Pará, poderá, garantida a defesa prévia, aplicar à licitante vencedora as seguintes sanções:

- a) Advertência, nas hipóteses de faltas leves, assim entendidas aquelas que não acarretem prejuízos para o TRE/PA;
- b) Multa compensatória de até 10% (dez por cento) sobre o valor global da Ata de Registro de Preços, na hipótese de recusa em assinar a Ata de Registro de Preços ou do contrato, na hipótese de recusa em assinar o instrumento de contrato;
- c) Multa compensatória de até 10% (dez por cento) sobre o valor global do respectivo material, na hipótese de recusa em receber a Ordem de Fornecimento e/ou de Serviço;
- d) Multa compensatória de até 10% (dez por cento) sobre o valor global do respectivo material, na hipótese de inexecução parcial ou total da obrigação.

19.3. Pelo atraso injustificado na execução do contrato, a CONTRATANTE deverá, garantida a defesa prévia, aplicar à licitante vencedora multa moratória de 0,2% (dois décimos por cento) por dia de atraso na entrega do material e/ou conclusão do serviço contratado, tomando por base o valor global do respectivo material, limitado a 10% (dez por cento).

19.4. O atraso injustificado na execução do contrato por período superior a 30 (trinta) dias, bem como deixar de manter todas as condições de habilitação, poderá ensejar a rescisão do contrato.

19.5. As multas aplicadas serão descontadas dos créditos da contratada ou, na impossibilidade, recolhidas no prazo de até 15 (quinze) dias, a contar da data da comunicação oficial para pagamento. Em caso de não recolhimento, o valor será cobrado judicialmente, consoante o disposto no § 3º do art. 86 e § 1º do art. 87 da Lei nº 8.666/93, acrescida de juros moratórios de 0,5% (meio por cento) ao mês e correção monetária pelo Índice de Preços ao Consumidor Amplo Especial – IPCA-E, nos termos art. 27 da Lei nº 9.069/95, c/c o art. 3º da Lei nº 10.192/2001.

19.6. Os prazos de adimplemento das obrigações contratadas admitem prorrogação nos casos e condições especificados no § 1º do art. 57 da Lei 8.666/93, e a solicitação dilatória deverá ser recebida contemporaneamente ao fato que a ensejar.

19.6.1. O pedido de prorrogação do prazo de execução não terá efeito suspensivo e deverá ser encaminhado por escrito, antes de expirado o prazo contratual, anexando-se documento comprobatório do alegado pela Contratada, competindo ao(a) Secretário(a) de Administração a concessão da prorrogação pleiteada.

19.7. Compete ao Diretor-Geral a apreciação e aplicação das penalidades previstas no item 19 e subitens, facultada a defesa do interessado, no prazo de 05 (cinco) dias úteis, contados da sua notificação.

19.8. Da aplicação das penalidades previstas no item 19 e subitens caberá recurso, no prazo de 05 (cinco) dias úteis, contados da notificação, que será dirigido à autoridade superior, por intermédio da que praticou o ato, a qual poderá reconsiderar a sua decisão, ou, fazê-lo subir devidamente informado.

19.9. As sanções de multa poderão ser aplicadas juntamente com as demais penalidades previstas neste Edital.

19.10. As penalidades aplicadas serão obrigatoriamente registradas no SICAF.

19.11. As Sanções acima descritas também se aplicam aos integrantes do Cadastro Reserva que, convocados, não honrarem o compromisso assumido, sem justificativa ou com justificativa recusada pela Administração Pública.

20 - DA ANULAÇÃO E REVOGAÇÃO

20.1. A autoridade competente para determinar a contratação poderá revogar a licitação em face de razões de Interesse Público, derivadas de fato superveniente devidamente comprovado, pertinente e suficiente para justificar tal conduta, devendo anulá-la por ilegalidade, de ofício ou por provocação de qualquer pessoa, mediante ato escrito e fundamentado.

20.2. A anulação do procedimento licitatório induz à da Ata de Registro de Preços.

20.3. As licitantes não terão direito à indenização em decorrência da anulação do procedimento licitatório, ressalvado o direito do contratado de boa-fé de ser ressarcido pelos encargos que tiver suportado no cumprimento do contrato.

20.4. No caso de desfazimento de processo licitatório, fica assegurado o direito ao contraditório e à ampla defesa.

21 - DOS ANEXOS

21.1. Integram este Edital, independente de transcrição, os seguintes Anexos:

- a) Anexo I – Termo de Referência;
- b) Anexo II – Minuta da Ata de Registro de Preços;
- c) Anexo III – Minuta de Contrato.

22 - DAS DISPOSIÇÕES FINAIS

- 22.1. Nenhuma indenização será devida às licitantes pela elaboração e/ou apresentação de documentação relativa ao presente pregão.
- 22.2. Na contagem de todos os prazos estabelecidos neste Edital excluir-se-á o dia de início e incluir-se-á o do vencimento, e considerar-se-ão os dias consecutivos, exceto quando for explicitamente disposto em contrário.
- 22.3. Só se iniciam e vencem os prazos referidos acima em dia de expediente neste Tribunal.
- 22.3.1. Se o vencimento cair em dia que não houver expediente neste Tribunal, os prazos de que trata o subitem 22.2 serão prorrogados para o primeiro dia útil seguinte.
- 22.4. O resultado desta licitação será divulgado no sítio <https://www.gov.br/compras/pt-br> e publicado na Imprensa Oficial.
- 22.5. O(s) contrato(s) advindo(s) do objeto deste Edital poderá(ão) sofrer acréscimos ou supressões de até 25% (vinte e cinco por cento), de conformidade com o artigo 65, da Lei n.º 8.666/93, sendo que as supressões poderão exceder este percentual, caso haja acordo entre as partes, conforme preconiza o § 2º do referido artigo.
- 22.6. É vedada a subcontratação para o objeto desta licitação.
- 22.7. Em caso de discrepância entre os Anexos e o Edital, prevalecerá o disposto no instrumento convocatório.
- 22.8. A indicação do lance vencedor, a classificação dos lances apresentados e demais informações relativas à sessão pública virtual deste Pregão constarão em ata divulgada no sistema eletrônico.
- 22.9. Para todas as referências de tempo contidas neste Edital será observado o horário de Brasília (DF) e, dessa forma, serão registradas no sistema eletrônico e na documentação relativa ao certame.
- 22.10. Maiores informações pelo telefone (91) 3346-8000.
- 22.11. O horário ordinário de recebimento e protocolização de documentos neste Regional é das 8h às 15h, conforme Portaria nº 11.109/2010 – SA (TRE-PA).
- 22.12. As controvérsias decorrentes deste contrato serão dirimidas no foro da Seção Judiciária de Belém, Capital do Estado do Pará, pela Justiça Federal, nos termos do art. 109, I, da Constituição Federal.

ANEXO I - TERMO DE REFERÊNCIA

OBS: No momento de cadastrar os itens no sistema eletrônico, as especificações correspondentes aos códigos (CATMAT / CATSER) disponíveis para cadastro nem sempre coincidem com as especificações ou unidades de medida dos bens ou serviços desejados. Portanto, havendo divergência entre as especificações constantes no sistema eletrônico e as contidas neste Termo de Referência, prevalecerão estas.

1. OBJETO

1.1. OBJETO DA CONTRATAÇÃO

A presente licitação tem por objeto o registro de preços para eventual e futura aquisição de solução de *Web Application Firewall* (WAF) e balanceamento de carga, incluindo prestação de serviços de instalação e configuração, treinamento especializado e serviço de operação assistida, com garantia técnica de 60 (sessenta) meses, de acordo com as especificações e quantitativos previstos neste Termo de Referência.

1.2. VALIDADE DA ATA: A Ata de Registro de Preços a ser gerada terá validade de 12 (doze) meses a partir da data da assinatura.

1.3 Farão parte deste Registro de Preços, como órgãos participantes, os seguintes Tribunais Regionais Eleitorais - TREs, os quais serão responsáveis pelas suas respectivas contratações: TRE-RJ, TRE-SP, TRE-SE, TRE-PR, TRE-TO, TRE-DF, TRE-PB, TRE-PE, TRE-AM, TRE-SC, TRE-AC, TRE-MS, TRE-RN, TRE-CE, TRE-ES, TRE-RO, TRE-AP e TRE-GO.

1.4. Justificativa para o agrupamento de itens

1.4.1. O agrupamento dos itens do objeto do presente instrumento em lote, tem por objetivo a padronização da contratação uma vez que os itens agrupados possuem a mesma natureza técnica, o que resulta ainda na otimização de recursos humanos e financeiros no desenvolvimento das atividades relacionadas à gestão contratual, uma vez que o gerenciamento de número variado de fornecedores traz ineficiência e custo na gestão e fiscalização da contratação.

1.4.2. Além disso, em razão da complexidade da solução, a possibilidade do parcelamento torna o contrato técnica, econômica e administrativamente inviável ou provoca a perda de economia de escala. Neste sentido, justifica-se o agrupamento em lote, uma vez que entendemos ser a opção mais vantajosa à administração e satisfatória do ponto de vista da eficiência técnica, por manter a qualidade do projeto, haja vista que o gerenciamento e execução técnica permanece todo o tempo a cargo de um mesmo fornecedor.

1.4.3. Nesse diapasão, as vantagens seriam o maior nível de controle pela Administração na execução da prestação de serviços, a maior facilidade no cumprimento do cronograma preestabelecido, a observância dos prazos de entrega do objeto, concentração da responsabilidade pela execução a cargo de um fornecedor e melhor garantia no acompanhamento dos resultados, para o objeto estabelecido neste Termo de Referência.

1.4.4. Isto posto, o agrupamento em lote visa garantir a compatibilidade técnica e operacional entre os componentes da solução, visto que haverá integração entre software e hardware existente no TRE-PA, serviços prestados, a contratação será realizada através de um único lote.

2. FUNDAMENTAÇÃO DA CONTRATAÇÃO

2.1. DA JUSTIFICATIVA

Com o crescimento dos ataques cibernéticos e espionagem virtual aos quais as empresas privadas e os órgãos da administração pública, especialmente o judiciário, têm sido vítimas, torna-se urgente a necessidade de adoção de mecanismos de segurança da informação e a utilização de recursos de inspeção e proteção do tráfego de dados que auxiliem, de forma proativa, a prevenção e proteção dos sistemas, ante às vulnerabilidades encontradas em diversos vetores – redes (perímetro), sistemas e aplicativos, servidores de aplicação, e infraestrutura de orquestradores de containers.

Eventos recentes de ataques cibernéticos contra órgãos do Poder Judiciário demonstram o potencial desses atacantes e a necessidade cada vez maior de implementar ações preventivas, detectivas e corretivas, de forma organizada e colaborativa para minimizar os riscos e reduzir os impactos às organizações. No Brasil, a escalada de ataques cibernéticos motivou a cúpula do Poder Judiciário, por meio do CNJ, a criar o Comitê de Segurança Cibernética do Poder Judiciário - Portaria CNJ Nº 242/2020. Os normativos publicados pelo Conselho Nacional de Justiça impõem diretrizes e novas responsabilidades quanto à segurança da informação e proteção de dados, além de um conjunto de controles e atividades técnicas que tem o objetivo de estabelecer um novo paradigma de segurança cibernética para os Órgãos do Poder Judiciário.

Por estes motivos, uma das necessidades urgentes da Justiça Eleitoral é na adoção de mecanismos de segurança da informação e a utilização de recursos de inspeção e proteção do tráfego de dados que auxiliem, de forma proativa, a prevenção das vulnerabilidades encontradas em diversos vetores – redes (perímetro), sistemas de mensagens eletrônicas (e-mail), sistemas e aplicativos, servidores de aplicação, e infraestrutura de orquestradores de containers.

A atenção relativa à segurança deve ser dispensada não somente aos sistemas informatizados, mas também às informações que esses sistemas recebem, armazenam, processam, divulgam e descartam. Na atualidade, as informações, que são consideradas patrimônio para as organizações, estão sob constantes riscos, o que indica que os investimentos para a proteção desses ativos precisam ser compatíveis com a sua importância, a complexidade dos ataques e o nível de exposição ao risco. Com isso, a Segurança da Informação tornou-se um ponto crucial para a sobrevivência e credibilidade das instituições.

A Resolução TSE nº 23.644/2021, que dispõe sobre a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral, instituiu como princípio norteador a garantia da disponibilidade, integridade, confidencialidade, autenticidade, irretratabilidade e audibilidade das informações produzidas, recebidas, armazenadas, tratadas ou transmitidas pelos órgãos da Justiça Eleitoral, no exercício de suas atividades e funções. Deste modo, o conjunto de orientações que fundamentam a Resolução TSE nº 23.644/2021 estão em consonância com o objetivo dessa contratação

Neste cenário, a Justiça Eleitoral trata diariamente um grande volume de dados sensíveis, necessitando proteger e garantir a confidencialidade, disponibilidade e integridade destas informações. Assim, com a ampliação da disponibilização das soluções baseadas em serviços e protocolos que constituem a Web, principalmente, HTTP (HyperText Transfer Protocol) e HTTPS (HyperText Transfer Protocol Secure), tanto para acessos externos e internos, os aplicativos da Web passaram a suportar uma ampla gama de funções críticas em diversos sistemas que sustentam os negócios, incluindo sistemas de recursos humanos, transparência e consulta processual, sistemas que suportam processos administrativos e judiciais, dentre outros. Estes meios, uma vez vulneráveis, tornaram-se uma brecha para ataques, pois os hackers não só podem invadir e roubar os dados das organizações por meio de e-mails maliciosos, programas infectados ou links duvidosos, como também oferecer perigo por meio do tráfego online até o site ou aplicativo corporativo. Torna-se necessário a ampliação da segurança, uma vez que os sistemas online podem conter potenciais vetores que se tornam alvos para a exploração de falhas, resultando nos conhecidos ataques cibernéticos

Pelo exposto, é necessária a contratação de uma solução que possa, de forma customizada ao ambiente, interceptar e mitigar o risco inerente aos sistemas. O alvo dos atacantes geralmente são vulnerabilidades em sistemas desatualizados, legados ou com falhas no desenvolvimento. Por meio dessas brechas, são realizados diversos tipos de ataques, visando à espionagem, ao vazamento de dados, ao roubo ou sequestro de informações, ou ainda à quebra de integridade e disponibilidade do ambiente.

Além do risco de vazamento de dados sensíveis, existe a preocupação de que a sociedade perca a confiança nos serviços disponibilizados, entre outras inúmeras consequências à imagem do Tribunal. Para que seja alcançado o nível de segurança exigido nos dias atuais, é necessário investir em processos, sistemas e conhecimento específicos contra ameaças avançadas.

Diante disso, Estratégia Nacional de Cibersegurança TSE e TREs (2021 a 2024), no Eixo Estruturante E3: Ferramentas Automatizadas (Ferramentas de Segurança de Borda), apontou a necessidade de contratação e implantação de solução de segurança WAF que permita realizar a proteção das aplicações da Internet/Intranet. A solução WAF, ou Firewall de Aplicação Web, é uma solução que fica entre o site ou aplicativo e o restante da internet e a rede interna, funcionando como uma barreira que bloqueia e protege o ambiente de aplicações contra ataques de Hackers, Spammers, DDoS, Injeções SQL, proteção contra captura de dados sensíveis e roubo de credenciais, prevenção à atividade de robôs (bots) maliciosos e muito outros tipos de ataques cibernéticos conhecidos.

Adicionalmente, considerando a necessidade de redução da complexidade da operação e a consolidação dos serviços para as aplicações, bem como o crescente uso de soluções e arquiteturas de software baseadas em contêineres, torna-se necessário que a solução pretendida inclua solução de balanceamento de carga e que a mesma seja integrada ao ambiente de contêineres, visando equalizar a distribuição de carga de acessos aos sistemas, tanto em ambiente interno quanto externo, tanto no ambiente das aplicações modernas quanto das aplicações legadas, nos diversos servidores de aplicação disponíveis na infraestrutura da Justiça Eleitoral, garantindo os requisitos necessários de segurança, desempenho e disponibilidade, principalmente, para sistemas críticos.

2.2. MOTIVAÇÃO DA CONTRATAÇÃO E NECESSIDADES DE NEGÓCIO

2.2.1. Com base nas diretrizes definidas na Estratégia Nacional de Cibersegurança, definidas pelo Tribunal Superior Eleitoral (TSE), vários investimentos em Tecnologia da Informação e Comunicação (TIC) estão sendo realizados para modernizar sua infraestrutura de TIC, com a finalidade mitigar o risco de ataques cibernéticos.

2.2.2. Dessa forma, visando alinhamento estratégico e ganho em escalabilidade, disponibilidade, confiabilidade na entrega dos serviços prestados à sociedade, existe a necessidade de contratação de solução de Web Application Firewall (WAF), que, dentre outras funções, realize a proteção e o balanceamento tráfego de aplicações.

2.2.3. O balanceamento de aplicações, que permite o aumento da disponibilidade, fazendo com que os acessos sejam distribuídos entre os recursos de infraestrutura, de maneira a otimizar seu uso.

2.2.4. A função de proteção das aplicações (mecanismo de segurança), realiza a interceptação, inspeção e processamento das requisições entre o cliente e a aplicação. A partir de um conjunto de regras, o WAF classifica as requisições em maliciosas (que são geralmente bloqueadas) e não-maliciosas, isto é, que são encaminhadas até a aplicação, objetivando garantir uma camada de proteção adequada aos sistemas e dados armazenados no Data Center do Tribunal.

2.2.5. Propõe-se, para tanto, a aquisição de Solução de Segurança da Informação – Firewall de Aplicação Web (WAF), visando à segurança e ao bom desempenho das atividades no âmbito desta Justiça Especializada. Conforme exposto, a aquisição fundamenta-se em razão da necessidade de mitigar os inúmeros riscos inerentes aos sistemas informatizados disponibilizados no Portais Internet e Intranet do Tribunal e, conseqüentemente, aumentar a confiabilidade, integridade e a disponibilidade dos serviços oferecidos ao público interno e à sociedade, segundo as melhores práticas do mercado de segurança da informação.

2.2.6. A motivação da contratação se dá, portanto, com base nas seguintes necessidades:

- No quesito segurança, pelo oferecimento de uma camada adicional de defesa, protegendo os servidores que hospedam aplicações Web, e executando funções de segurança de proteção dos servidores internos contra ataques por usuários da internet;
- No quesito performance, pela melhoria de acesso às aplicações dos sistemas administrativos e judiciais, através do balanceamento de carga;
- Ampliar o controle de perímetro, por meio da inspeção e análise contínuo de tráfego das aplicações;
- Aprimorar os mecanismos de monitoramento e detecção de ataques;
- Proporcionar a prevenção e mitigação de Ameaças Cibernéticas;
- Contribuir para a redução da superfície de ataques cibernéticos da justiça eleitoral.

2.3. OBJETIVOS A SEREM ALCANÇADOS POR MEIO DA CONTRATAÇÃO

2.3.1. Garantir que o acesso lógico aos ativos seja gerenciado e protegido, por meio de mecanismos de segurança de perímetro;

2.3.2. Tornar a infraestrutura da Justiça Eleitoral mais segura e confiável;

2.3.3. Prover resiliência ao ambiente de produção;

2.3.4. Assegurar a redundância adequada ao porte do parque tecnológico do Regional.

2.4. OBJETIVO DA CONTRATAÇÃO

2.4.1. Trata-se de contratação de empresa para fornecimento de solução de Web Application Firewall (WAF), na modalidade de Appliance Virtual e Físico, acrescido de licenciamento adicional, serviços de configuração, instalação, transferência de conhecimento e Operação Assistida.

2.5. Alinhamento Estratégico

I - PEJEPA 2021/2026 - Fortalecimento da Estratégia Nacional de TIC e de Proteção de Dados

- Índice de continuidade
 - Abrange a medição do percentual de disponibilidade e desempenho dos serviços de rede e sistemas informatizados.
- Índice de cumprimento de requisitos de Proteção de Dados
 - Mede o percentual de cumprimento da implantação dos requisitos relacionados à Proteção e Segurança de Dados.

II - Planejamento Estratégico de TI (PETI) 2019-2022.

- Perspectiva Recursos / Objetivo Estratégico 2 - Garantir a Modernização dos Serviços e Infraestrutura de TI
 - Indicadores Estratégicos:
 - 2.1 Índice de disponibilidade de serviços de rede e sistemas essenciais de TI TRE-PA
 - 2.2 Índice de indisponibilidade para acesso à rede da Justiça Eleitoral

III - Outros Referenciais Estratégicos

- Estratégia Nacional de Cibersegurança - 2021 a 2024 (TSE e TREs) - evento 1370070
 - Eixo Estruturante E3: Ferramentas Automatizadas
 - **item ID_F05 S / WAF - WEB APP. FIREWALL - INTRANET**
- Resolução Nº 396 de 07/06/2021, Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ)
 - Portaria Nº 162 de 10/06/2021 - Protocolos e Manuais (ENSEC-PJ).

2.6. Referências aos Estudos Preliminares

- Evento 1483788 - Processo SEI 0008981-46.2021.6.14.8000

2.7. Referências Legais

- Portaria nº18456/2019, estabelece as diretrizes para a Gestão de Ativos de Tecnologia da Informação e Comunicações e institui o processo de gestão de configuração e ativos de TIC no âmbito do TRIBUNAL REGIONAL ELEITORAL DO PARÁ – TRE-PA;
- Resolução CNJ Nº 182/2013, dispõe sobre diretrizes para as contratações de Solução de Tecnologia da Informação e Comunicação pelos órgãos submetidos ao controle administrativo e financeiro do Conselho Nacional de Justiça (CNJ);
- Resolução CNJ nº 370/2021, institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);
- Resolução CNJ nº 396, de 7 de junho de 2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);
- LGPD – Lei Geral de Proteção de Dados (Lei no 13.709/2018) e Marco Civil da Internet Lei no 12.965/2014);
- Resolução TSE Nº 23.644, de 1º de julho de 2021, Dispõe sobre a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;
- Lei 8.666/1993, regulamenta o art. 37, inciso XXI, da Constituição Federal, institui normas para licitações e contratos da Administração Pública e dá outras providências.
- Instrução Normativa Nº 1, de 4 de abril de 2019. Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal;
- Decreto 9.488/2018, altera o Decreto nº 7.892, de 23 de janeiro de 2013, que regulamenta o Sistema de Registro de Preços previsto no art. 15 da Lei nº 8.666, de 21 de junho de 1993, e o Decreto nº 7.579, de 11 de outubro de

2011, que dispõe sobre o Sistema de Administração dos Recursos de Tecnologia da Informação - SISF, do Poder Executivo federal;

- Estratégia Nacional de Cibersegurança TSE e TREs (2021 a 2024), no Eixo Estruturante E3: Ferramentas Automatizadas (Ferramentas de Segurança de Borda), apontou a necessidade de contratação e implantação de solução de segurança WAF que permita realizar a proteção das aplicações da Internet/Intranet.

2.8. Classificação do Objeto

2.8.1. Objeto associado à contratação é considerado comum, pois apresenta padrões de desempenho e qualidade que podem ser objetivamente definidos pelo edital, por meio de especificações usuais de mercado.

2.9. Relação entre a demanda prevista e a quantidade a ser contratada

2.9.1. A contratação tem por objetivo assegurar a proteção de aplicações WEB e informações sensíveis armazenadas nos servidores em produção Tribunal por meio solução de Web Appliaction Firewall. Para tanto, devido a necessidade da contratação, as quantidades abaixo foram consolidadas através de consulta da estimativa de demanda realizada com Tribunais Regionais Eleitorais, para compor o projeto em sua totalidade, com vistas a contratação da solução, serviços de implantação e treinamento, garantia técnica, bem como a necessidade de complementação de licenças da solução.

A tabela a seguir apresenta o demonstrativo consolidado dos quantitativos levantados junto ao TRE-PA e aos TREs partícipes da Ata de Registro de Preços, conforme tabela constante do item 5.9 deste Termo de Referência.

DEMANDA EXISTE	QTDE	DESCRIÇÃO DA SOLUÇÃO DE TI A SER CONTRATADA	JUSTIFICATIVAS
PROTEÇÃO DE APLICAÇÕES WEB PUBLICADAS NA INTERNET/INTRANET, HOSPEDADAS NO DATA CENTER DO TRIBUNAL	28	CLUSTER/SOLUÇÃO DE PROCEÇÃO CAMADA 7 PARA APLICAÇÕES WEB, FIREWALL(WAF), DO TIPO APPLIANCE VIRTUAL.	Cluster de proteção (2 appliances) das aplicações WEB hospedadas no ambiente de produção (Data Center) do Tribunal, visando mitigar os riscos de ataque cibernético, com Garantia e suporte técnico do fabricante, período de 60(sessenta) meses, necessárias à manutenção da disponibilidade da solução.
	20	CLUSTER/SOLUÇÃO DE PROCEÇÃO CAMADA 7 PARA APLICAÇÕES WEB, FIREWALL(WAF), DO TIPO APPLIANCE FÍSICO.	<p><i>* O fornecedor deverá prover a solução na modalidade de appliance Físico e Virtual, em razão da necessidade de cara Regional partícipe da Ata RP.</i></p> <p><i>** Deverão ser fornecidas 2(duas) unidades da solução, em cada modalidade, para configuração do cluster, em razão da redundância do serviço.</i></p>
LICENCIAMENTO EXPANSÃO DE CAPACIDADE	28	CAPACIDADE ADICIONAL PARA SOLUÇÃO EM FIREWALL DE APLICAÇÕES WEB	Capacidade adicional para solução em Firewall de Aplicações WEB, visando a expansão de capacidade da Taxa de transferência (throughput) da solução (específico para o ITEM 1 da solução.
SERVIÇO DE INSTALAÇÃO E REPASSE DE CONHECIMENTO HANDS-ON	20	SERVIÇO DE INSTALAÇÃO E REPASSE DE CONHECIMENTO HANDS-ON	Implantação da solução, incluindo instalação e configuração no ambiente do Tribunal e repasse técnico-operacional básico da solução.

	90	TREINAMENTO ESPECIALIZADO	Capacitação da equipe técnica para administração da solução, por meio de treinamento.
SUPERVISÃO DA SOLUÇÃO EM PRODUÇÃO APÓS A IMPLANTAÇÃO	19	OPERAÇÃO ASSISTIDA	Serviço de operação assistida.

Tabela 2 - Levantamento da demanda e quantidades e solução/serviço de TI a ser contratado.

2.9.2. Além disso, foram mapeadas as seguintes premissas gerais para atendimento da demanda:

- A Solução deverá possuir gerenciamento e armazenamento dos dados na rede local do tribunal, com appliances próprios localizados e instalados na infraestrutura do cliente (on-premise);
- A solução deve ser licenciada para uso perpétuo. As funcionalidades da solução devem permanecer ativas após o período de garantia mesmo que desatualizadas e com todas as atualizações e assinaturas que forem disponibilizadas até data final do período que foram aplicadas ou instaladas na solução;
- A CONTRATADA deverá ofertar a solução na modalidade de Appliance Físico e Appliance Virtual;
- A contratação deverá fornecer implantação da solução no ambiente do Tribunal e treinamento EAD;
- A CONTRATADA deverá ofertar Garantia do Fabricante por 60(sessenta) meses. A garantia refere-se ao período oficial de suporte da solução, fornecido por seu fabricante, compreendendo o fornecimento de atualizações e correções durante todo o ciclo de vida da versão fornecida do sistema operacional.

3 ESPECIFICAÇÃO TÉCNICA E QUANTIDADE

LOTE ÚNICO			
ITEM	DESCRIÇÃO	UNIDADE DE MEDIDA	QUANT.
1	FORNECIMENTO DE SOLUÇÃO DE WEB APPLICATION FIREWALL(WAF), DO TIPO APPLIANCE VIRTUAL, COM GARANTIA DE 60(SESENTA) MESES.	UN	28
<p>3.1. A SOLUÇÃO DE WEB APPLICATION FIREWALL – WAF</p> <p>3.1.1. Requisitos mínimos da solução:</p> <p>3.1.2. A Solução de WEB APPLICATION FIREWALL- (WAF) deverá ser instalado no data center do CONTRATANTE.</p> <p>3.1.3. A solução deverá ser do tipo Appliance virtual, compatível com os virtualizadores hypervisor VMWARE ESXi 6.5+, KVM, CITRIX XENSERVER. e Hyper-V; devendo observar os seguintes requisitos mínimos:</p> <p>3.1.3.1. Deve suportar a configuração de, no mínimo, 8(oito) vCPUs;</p> <p>3.1.3.2. Deve suportar a configuração de, no mínimo, 8(oito) interfaces de Rede;</p> <p>3.1.3.3. Deve suportar a configuração de um storage de, no mínimo, 1 (um) TB;</p>			

- 3.1.3.4. Deve suportar a configuração de, no mínimo, 64(sessenta e quatro) GB de memória RAM.
- 3.1.4. A solução deve ser licenciada para uso perpétuo. As funcionalidades da solução devem permanecer ativas após o período de garantia mesmo que desatualizadas e com todas as atualizações e assinaturas que forem disponibilizadas até data final do período que foram aplicadas ou instaladas na solução.
- 3.1.5. A Solução deverá possuir gerenciamento e armazenamento dos dados na rede local do tribunal, com appliances próprios localizados e instalados na infraestrutura do cliente (on-premise)
- 3.1.6. Capacidade de inspecionar no mínimo 01 Gbps (Um gigabit por segundo) de tráfego web em camada 7;
- 3.1.7. Admitir no mínimo 30.000 (trinta mil) novas conexões por segundo em camada 7;
- 3.1.8. Admitir no mínimo 900 (novecentas) transações por segundo (TPS) SSL com chaves RSA 2048 bits;
- 3.1.9. Suportar 2.000.000 (dois milhões) de conexões concorrentes em camada 4;
- 3.1.10. Suportar e garantir a instalação em ambiente de alta disponibilidade;
- 3.1.11. Deve permitir a configuração da solução em alta disponibilidade, permitindo o funcionamento em cluster do tipo ativo-passivo e ativo-ativo.
- 3.1.12. A solução deve suportar mais do que dois elementos no cluster para sincronização de configuração de forma nativa a fim de permitir escalabilidade no futuro.
- 3.1.13. Implementar a sincronização entre os equipamentos redundantes, assegurando que não haverá "downtime" e queda de sessões em caso de falha de uma das unidades.
- 3.1.14. Deve possuir redundância de dispositivos, de maneira que, em caso de falha de um dos equipamentos, o estado de todas as conexões seja remanejado para o equipamento redundante, preservando o estado original de todas as tabelas de conexões e de persistência.
- 3.1.15. O equipamento deve permitir a sincronização das configurações de forma automática.
- 3.1.16. Caso seja necessária uma interligação entre os equipamentos, a CONTRATADA será integralmente responsável por tal interligação, garantindo a performance necessária para o atendimento da solução.
- 3.1.17. O equipamento, quando habilitado para mais de uma função (Balanceamento, DNS, Web Application Firewall, etc), deverá permitir a definição da importância da função para cada tipo de funcionalidade ou realizar tal tarefa de forma automática visando o bom funcionamento do equipamento;
- 3.1.18. Possuir capacidade para gerenciar os recursos disponíveis de acordo com as funções habilitadas nos equipamentos SLB, GSLB, WAF, etc.
- 3.1.19. Fornecer recurso para o transporte de múltiplas VLANs por uma única porta (ou por um conjunto agregado de portas) utilizando o protocolo 802.1q;
- 3.1.20. Analisar e proteger tráfego HTTP/1.0, HTTP/1.1, HTTP/2.0 e/ou HTTP/3;
- 3.1.21. Possuir suporte a IPv6;
- 3.1.22. A solução deve permitir o encapsulamento, em camada 3, do tráfego entre o balanceador e o servidor para tráfego IPv4 e IPv6, quando o balanceamento é realizado apenas em direção ao servidor, onde a resposta do servidor real é enviada diretamente ao cliente;
- 3.1.23. Deve suportar, no mínimo, 1000 VLANs simultaneamente;
- 3.1.24. Implementar o SNTP (Simple Network Time Protocol) ou NTP (Network Time Protocol);
- 3.1.25. Possuir suporte à funcionalidade de VXLAN, essencial para integração com o ambiente de virtualização (Software Defined Network).
- 3.1.26. Assinar cookies digitalmente e editar endereços de URL ("URL Rewriting");
- 3.1.27. O equipamento deverá permitir a sincronização das configurações:
 - 3.1.27.1.1. De forma automática;
 - 3.1.27.1.2. Manualmente, forçando a sincronização apenas no momento desejado;
- 3.1.28. Permitir a configuração das interfaces de alta disponibilidade do cluster (heartbeat), com opções para:
 - 3.1.28.1.1. Compartilhar a rede de heartbeat com a rede de dados;
 - 3.1.28.1.2. Utilizar uma rede exclusiva para o heartbeat.
- 3.1.29. Permitir que regras customizadas em linguagem aberta possam ser utilizadas para customizar a distribuição dinâmica de tráfego e aumentar a proteção contra ataques;
- 3.1.30. A solução deve possuir linguagem de programação open-source que permita a manipulação do tráfego de entrada e saída, viabilizando assim a alteração de parâmetros no cabeçalho e no corpo das mensagens.
- 3.1.31. Essa linguagem de programação deve permitir a importação de pacotes, garantindo assim que a agilidade e flexibilidade no compartilhamento dos scripts.
- 3.1.32. Permitir a criação de políticas através de interface gráfica web para manipulação de tráfego através de lógica para pelo menos os seguintes operadores:
- 3.1.33. GEOIP, http-basic-auth, http-cookie, http-header, http-host, http-method, http-referer, http-set-cookie, http-status, http-uri e http-version
- 3.1.34. A solução deve possuir políticas de uso de senhas administrativas tais como: nível de complexidade, período de validade e travamento de conta devido a erros múltiplos de login de forma nativa ou no mínimo integrado a uma base Active Directory ou LDAP ou tacacs;
- 3.1.35. Deve implementar configuração de endereçamento IP estático ou dinâmico (DHCP/BOOTP) para a interface de gerenciamento;
- 3.1.36. Permitir acesso in-band via SSH
- 3.1.37. Possuir console de administração com interface gráfica remota segura atendendo os seguintes requisitos:
 - 3.1.37.1.1. Permitir a definição de diferentes níveis de administração, no mínimo, um nível completo e outro

somente de visualização de configurações e logs;

3.1.37.1.2. Permitir a replicação de configurações e a aplicação de atualização de softwares para os elementos dos nós do cluster;

3.1.38. Manter internamente múltiplos arquivos de configurações do sistema;

3.1.39. Utilizar SCP ou HTTPS como mecanismo de transferência de arquivos de configuração e Sistema Operacional;

3.1.40. Os usuários de gerência deverão poder ser autenticados em bases remotas. No mínimo RADIUS, LDAP e TACACS+ deverão ser suportados;

3.1.41. Deverá ser possível associar aos usuários de bases externas como RADIUS, LDAP e TACACS+ o nível de acesso;

3.1.42. Possuir Interface Gráfica via Web;

3.1.43. Possuir auto-complementação de comandos na CLI;

3.1.44. Possuir ajuda contextual;

3.1.45. A Solução deve ter a capacidade de permitir a criação de MIBs customizadas ou ter suporte a snmpv1/v2/v3 para monitoramento do equipamento;

3.1.45.1. A solução deve possuir arquivo de MIBs e documento descrevendo os OIDs e o que é possível coletar utilizando SNMP;

3.1.46. A Solução deve ter suporte a sFlow;

3.1.47. Interface por linha de comando (CLI – Command Line Interface) que possibilite a configuração dos equipamentos;

3.1.48. Possuir, no mínimo, Três níveis de usuários na GUI – Super-Usuário, Usuário com permissões reduzidas, e usuário Somente Leitura;

3.1.49. A interface Gráfica deverá permitir a atualização do sistema operacional e/ou a instalação de patches ou Hotfixes sem o uso da linha de comando;

3.1.50. A interface gráfica deverá permitir a configuração de qual partição o equipamento deverá dar o boot;

3.1.51. Possuir um comando, via CLI, que mostre o tráfego de utilização das interfaces (bps e pps);

3.1.52. Suportar a rollback de configuração e imagem;

3.1.53. Possuir e fornecer geração de mensagens de syslog para eventos relevantes ao sistema;

3.1.54. Possuir configuração de múltiplos syslog servers para os quais o equipamento irá enviar as mensagens de syslog;

3.1.55. Possuir armazenamento de mensagens de syslog em dispositivo interno ao equipamento;

3.1.56. A interface Gráfica deverá permitir a reinicialização do equipamento;

3.1.57. Reinicialização do equipamento por comando na CLI;

3.1.58. Possuir recurso de gerência via SNMP e implementar SNMPv1, SNMPv2c e SNMPV3;

3.1.59. Possuir traps SNMP;

3.1.60. Caso a solução possua suporte a RMON, deverá possuir suporte a monitoração utilizando pelo menos 4 grupos: statistics, history, alarms e events.

3.1.61. Os logs de sistema devem ter a opção de ser armazenados internamente ao sistema ou em servidor externo;

3.1.62. Implementar Debugging: CLI via console e SSH;

3.1.63. Permite a criação de políticas diferenciadas por aplicação e por URL, onde cada aplicação e URL poderão ter políticas totalmente diferentes;

3.1.64. Permitir a criação de políticas diferenciadas por aplicação.

3.1.65. Deverá possuir uma funcionalidade de criação automática de políticas, para proteção DDOS e ataques zero-day onde a política de segurança é criada e atualizada automaticamente baseando-se no tráfego real observado à aplicação;

3.1.66. O perfil aprendido de forma automatizada pode ser ajustado, editado ou bloqueado;

3.1.67. Restringir métodos HTTP/ HTTPS permitidos, tipos ou versões de protocolos, tipos de caracteres e versões utilizadas de cookies;

3.1.68. Permitir as seguintes opções de implementação:

3.1.69. Monitoramento (sem bloqueio);

3.1.70. Proxy (reverso e transparente).

3.1.71. Permitir que novas políticas fiquem apenas monitorando o tráfego, sem bloqueá-lo, indicando caso aconteça algum evento;

3.1.72. Remover as mensagens de erro do conteúdo que será enviado aos usuários;

3.1.73. Em modo “monitoramento” (sem bloqueio), realizar análise e avaliação do tráfego, gerar relatórios com os dados analisados e simular bloqueios para efeito de avaliação;

3.1.74. Proteger contra-ataques automatizados, incluindo bots e web scraping, identificando comportamento não humano, navegadores operados por scripts ou qualquer outra forma que não operados por humanos;

3.1.75. Bloquear ataques aos servidores de aplicação, por meio dos seguintes recursos:

3.1.75.1. Identificação, isolamento e bloqueio de ataques sofisticados sem impactar nas transações das aplicações;

3.1.76. Possuir firewall XML integrado com suporte a filtro e validação de funções XML específicas da aplicação;

- 3.1.77. A solução deve suportar e fazer a proteção do tráfego de protocolo WebSocket.
- 3.1.78. Com a finalidade de proteger as aplicações, a solução deve suportar o uso de páginas de login AJAX/JSON tanto com configuração manual como descoberta automática.
- 3.1.79. Permitir a utilização de modelo positivo de segurança para proteger contra ataques às aplicações HTTP e HTTPS, além de proteção contra ataques conhecidos aos protocolos HTTP e HTTPS;
- 3.1.80. Quando detectada uma tentativa de ataque bloquear de imediato o tráfego ou a sessão;
- 3.1.81. Bloqueio com intermediação e interrupção da conexão;
- 3.1.82. Criação de políticas automáticas que bloqueiam o endereço IP que realizar violações;
- 3.1.83. Utilização de página HTML informativa e personalizável como HTTP Response aos bloqueios;
- 3.1.84. Configuração de políticas de bloqueio baseadas em requisição HTTP, endereço IP e usuário de aplicação;
- 3.1.85. Permitir apenas transações de aplicações validadas, o restante das transações deverá ser bloqueado, utilizando bloqueio por nível de aplicação baseado no contexto da sessão do usuário, com privilégios de autorização diferentes, entradas de usuários e tempo de resposta de aplicação;
- 3.1.86. Identificar e armazenar o ataque acontecido com detalhes, com as seguintes informações:
 - 3.1.86.1. Endereços IP que originaram os ataques;
 - 3.1.86.2. Horário do ataque;
 - 3.1.86.3. Nome do ataque;
 - 3.1.86.4. Qual campo foi atacado;
 - 3.1.86.5. Quantas vezes esse ataque foi realizado;
- 3.1.87. Possuir mecanismo de aprendizado automatizado capaz de identificar todos os conteúdos das aplicações, incluindo URLs, parâmetros URLs, campos de formulários, o que se espera de cada campo (tipo de dado, tamanho de caracteres, se é um campo obrigatório), cookies, ações SOAP e elementos XML; identificar e criar perfil de utilização dos aplicativos, inclusive desenvolvidos em Javascript, CGI, ASP e PHP;
- 3.1.88. O perfil aprendido de forma automatizada pode ser ajustado, editado ou bloqueado;
- 3.1.89. Identificar ataques baseados em:
 - 3.1.89.1. Assinaturas, com atualização periódica da base pelo fabricante;
 - 3.1.89.2. Regras;
 - 3.1.89.3. Perfis de utilização;
- 3.1.90. Deve possuir tecnologia para mitigação de DDoS em camada 7 baseado em análise comportamental, usando o aprendizado.
- 3.1.91. Não deve haver a necessidade de intervenção de usuário para configurar thresholds DoS pois esses valores devem ser auto-ajustáveis e adaptativos de acordo com mudanças.
- 3.1.92. A solução deve possuir a capacidade de capturar tráfego no formato TCP Dump relativos a ataques DoS L7, Web Scraping e força bruta permitindo uma análise mais aprofundada por parte do administrador.
- 3.1.93. Detectar ataques de força bruta por meio dos seguintes métodos:
- 3.1.94. Aumento do tempo de resposta da aplicação monitorada ou bloqueio temporário do atacante;
- 3.1.95. Quantidade de transações por segundo (TPS), monitorando a quantidade de transações por segundo por endereço IP.
- 3.1.96. Detectar ataques do tipo força bruta em que:
 - 3.1.96.1. O atacante solicita repetidamente o mesmo recurso;
 - 3.1.96.2. O atacante realiza repetidas tentativas não autorizadas de acesso;
 - 3.1.96.3. São utilizados ataques automatizados de login.
- 3.1.97. Detectar ataques do tipo força bruta que explorem:
 - 3.1.97.1. Controles de acesso da aplicação (Erro 401 – Unauthorized);
 - 3.1.97.2. Solicitações repetidas ao mesmo recurso, em qualquer parte/URL da aplicação;
 - 3.1.97.3. Aplicações WEB que não retornam o erro 401 por meio da identificação de expressão regular no retorno/página de erro da aplicação);
 - 3.1.97.4. Gerenciamento de sessão (muitas sessões de um único endereço IP ou a um range de Ips);
 - 3.1.97.5. Clientes automatizados (robôs, requisições muito rápidas);
 - 3.1.97.6. Permitir a criação de políticas diferenciadas por aplicação e por URL, onde cada aplicação e URL poderão ter políticas totalmente diferentes;
 - 3.1.97.7. Possuir mecanismo para criação dinâmica de política de segurança, com aprendizado automático de padrão de utilização da aplicação, realizado sobre o fluxo de tráfego bidirecional atravessando o equipamento;
 - 3.1.97.8. Possibilitar atualização de novas assinaturas para ataques conhecidos;
- 3.1.98. Apresentar proteção contra-ataques, como:
 - 3.1.98.1. Brute Force Login;
 - 3.1.98.2. Buffer Overflow;
 - 3.1.98.3. Cookie Injection;
 - 3.1.98.4. Cookie Poisoning;
 - 3.1.98.5. Cross Site Request Forgery (CSRF);
 - 3.1.98.6. Cross Site Scripting (XSS);
 - 3.1.98.7. Server Side Request Forgery (SSRF)
 - 3.1.98.8. Directory Traversal;

- 3.1.98.9. Forceful Browsing;
- 3.1.98.10. HTTP Denial of Service;
- 3.1.98.11. HTTP hidden field manipulation;
- 3.1.98.12. HTTP request smuggling;
- 3.1.98.13. HTTP Response Splitting;
- 3.1.98.14. Malicious Robots;
- 3.1.98.15. Parameter Tampering;
- 3.1.98.16. Remote File Inclusion Attacks;
- 3.1.98.17. Sensitive Data Leakage (Social Security Numbers, Cardholder Data, PII, HPI);
- 3.1.98.18. Session Hijacking;
- 3.1.98.19. SQL Injection;
- 3.1.98.20. Web Scraping;
- 3.1.98.21. Web server software and operating system attacks;
- 3.1.98.22. Web Services (XML) attacks;
- 3.1.99. Permitir configurar granularmente, por aplicação protegida, restrições de métodos HTTP permitidos, tipos ou versões de protocolos, tipos de caracteres e versões utilizadas de cookies;
- 3.1.100. Suportar os seguintes critérios de decisão para realizar bloqueio ou gerar alerta, sendo que uma política pode conter um ou mais critérios simultaneamente:
 - 3.1.100.1. Assinatura de ataque ou Ips de atacantes conhecidos;
 - 3.1.100.2. Código de response;
 - 3.1.100.3. Conteúdo da cookie;
 - 3.1.100.4. Conteúdo do cabeçalho;
 - 3.1.100.5. Conteúdo do payload;
 - 3.1.100.6. Hostname;
 - 3.1.100.7. IP de origem;
 - 3.1.100.8. Método HTTP;
 - 3.1.100.9. Número de ocorrências em determinado intervalo de tempo;
 - 3.1.100.10. Parâmetro;
 - 3.1.100.11. User-agent (navegador);
- 3.1.101. Deve proteger contra os seguintes ataque por meio de assinaturas seletivas:
 - 3.1.101.1. Ataques de negação de serviços automatizados;
 - 3.1.101.2. Worms e vulnerabilidades conhecidas;
 - 3.1.101.3. Requests em objetos restritos;
- 3.1.102. Deve proteger contra ataques SSRF (Server Side RequestForgery);
- 3.1.103. A solução oferecida deverá possuir proteção contra ataques, disponibilizando acesso a base de assinaturas e atualizações periódicas ate o fim do contrato;
- 3.1.104. Ao atualizar ou adicionar uma nova assinatura, a solução deve automaticamente colocar essa assinatura em modo “staging” para evitar falsos positivos e não bloquear tráfego válido. Depois de um período a mesma deve automaticamente entrar em modo de bloqueio.
- 3.1.105. Deve permitir que possa ser especificado na política os tipos de arquivos que serão bloqueados (File Types);
- 3.1.106. A solução deve permitir a inspeção de upload de arquivos para os servidores de aplicação, ou enviar para inspeção através do protocolo ICAP;
- 3.1.107. Deve possuir uma proteção proativa comportamental contra ataques automatizados por robôs e outras ferramentas de ataque;
- 3.1.108. Ao detectar uma condição de DDoS, assinaturas dinâmicas devem ser automaticamente criadas e implementadas em tempo real para proteção da aplicação;
- 3.1.109. A solução deve possuir proteção de DDoS L7 baseado em análise comportamental, sem precisar de nenhuma configuração manual;
- 3.1.110. Possuir método de mitigação de DoS L7 baseado em:
 - 3.1.110.1. Descarte de todas as requisições de um determinado IP e/ou país suspeito;
 - 3.1.110.2. CAPTCHA para suspeitos que ultrapassarem os thresholds;
 - 3.1.110.3. Defesa proativa contra Bot, através da injeção de um desafio no Browser ou via Javascript para detectar se é um usuário legítimo ou robô;
- 3.1.111. Deve aprender automaticamente o comportamento da aplicação e combinar o comportamento heurístico do tráfego, análise de dados e Machine Learning, com o stress do servidor de aplicação para determinar uma condição de DDoS;
- 3.1.112. Aprender o comportamento da aplicação:
 - 3.1.112.1. Campos, valores, cookies e URLs;
- 3.1.113. Políticas sugeridas somente devem ser aplicadas após um período configurável;
- 3.1.114. Inspeccionar e monitorar até a camada de aplicação, todo tráfego de dados HTTP, incluindo cabeçalhos, campos de formulários e conteúdo, além de inspecionar os requests e responses;
- 3.1.115. Realizar as checagens em todos os tipos de entrada de dados, como URLs, formulários, cookies, campos ocultos e parâmetros, consultas (query), métodos HTTP, elementos XML e ações SOAP;

- 3.1.116. Proteger contra mensagens XML e SOAP malformadas;
- 3.1.117. Utilizar o campo HTTP X-Forwarded-For sem modificar seu conteúdo de origem, permitindo a diferenciação em ambientes com NAT;
- 3.1.118. Remover as mensagens de erro do conteúdo que será enviado aos usuários;
- 3.1.119. Deverá permitir o bloqueio de robôs (bots) que acessam a aplicação através de detecção automática ou vir com lista dos principais robôs já pré configurada, inclusive para Robôs conhecidos do mercado, como por exemplo Google, Yahoo e Microsoft Bing, que deverão ser liberados por padrão.
- 3.1.120. Deverá permitir o cadastro de robôs que podem acessar a aplicação;
- 3.1.121. Deverá implementar proteção ao JSON (JavaScript Object Notation);
- 3.1.122. Implementar a segurança de web services, através dos seguintes métodos:
 - 3.1.122.1. Criptografar/Decriptografar partes das mensagens SOAP;
 - 3.1.122.2. Assinar digitalmente partes das mensagens SOAP;
 - 3.1.122.3. Verificação de partes das mensagens SOAP;
- 3.1.123. Deverá permitir o bloqueio de ataques de força bruta de usuário/senha em páginas de acesso (login) que protegem áreas restritas. Este bloqueio deve limitar o número máximo de tentativas e o tempo do bloqueio deverá ser configurável;
- 3.1.124. Deve encriptar dados e credenciais na camada de aplicação, sem ter a necessidade de atualizar a aplicação. Essas informações devem ser encriptadas para proteger o login e as credenciais dos usuários e com isso os dados da aplicação;
- 3.1.125. Deve proteger informações sensíveis e confidenciais da interceptação por terceiros, através da criptografia de dados quando ainda no browser do usuário. Deve proteger esses dados criptografados de malwares e keyloggers;
- 3.1.126. Deve ofuscar o nome de um parâmetro sensível da aplicação em caracteres randômicos. Esse nome de parâmetro deve ser mudado constantemente pela ferramenta para dificultar ataques direcionados;
- 3.1.127. Deverá possuir controle de fluxo por aplicação permitindo definir o fluxo de acesso de uma URL para outra da mesma aplicação. Dessa forma qualquer tentativa de acesso a um determinado site que não siga o fluxo passando pelas URLs pré-definidas deverá ser bloqueado como uma tentativa de acesso ilegal;
- 3.1.128. A solução deverá se integrar a soluções de análise (Scanner) de terceiros, de forma automática ou manual, como por exemplo Trustwave App Scanner (Cenzic), White Hat Sentinel, IBM AppScan, Qualys, QuotiumSeeker, HP Webspect, Tenable; com a capacidade de criar regras para proteção das vulnerabilidades encontradas na análise do Scanner.
- 3.1.129. A solução deve fornecer relatórios consolidados de ataques com pelo menos os seguintes dados:
 - 3.1.130.1. Resumo geral com as políticas ativas, anomalias e estatísticas de tráfego, Ataques DoS, Ataques de Força Bruta, Ataques de Robôs, Violações, URL, Endereços IP, Países, Severidade.
- 3.1.131. Deverá permitir o agendamento de relatórios a serem entregues por email;
- 3.1.132. Emitir os seguintes relatórios gráficos por:
 - 3.1.132.1. Política de segurança;
 - 3.1.132.2. Tipos de ataques;
 - 3.1.132.3. Violações;
 - 3.1.132.4. URL que foram atacadas;
 - 3.1.132.5. Endereços IP de origem;
 - 3.1.132.6. localização geográfica dos endereços IPs de origem;
 - 3.1.132.7. Severidade;
 - 3.1.132.8. Código de resposta;
 - 3.1.132.9. Métodos;
 - 3.1.132.10. Protocolos;
 - 3.1.132.11. Sessão;
- 3.1.133. Permitir a seleção de período para emissão dos relatórios,
- 3.1.134. Permitir a geração das seguintes informações, por período:
 - 3.1.134.1. Permitir auditoria detalhada das alterações de configuração efetuadas, indicando usuário, ação e horário;
 - 3.1.134.2. Informações estatísticas de quantidade de conexões completadas e bloqueadas;
 - 3.1.134.3. Informações estatísticas de fluxo de tráfego;
 - 3.1.134.4. Informações estatísticas de quantidade de sessões ou conexões;
- 3.1.135. Identificação, isolamento e bloqueio de ataques sofisticados para os protocolos: HTTP e HTTPS;
- 3.1.136. Deve possuir capacidade para definir que todo tráfego seja tunelado e permitir a utilização do protocolo padrão HTTPS com SSL como transporte, possibilitando a sua utilização com proxy HTTP e possibilitar utilização de encapsulamento
- 3.1.137. Deve possuir capacidade para definir servidor virtual em HTTPS com perfil cliente SSL/TLS padrão e redirecionar tráfego HTTP para HTTPS para um determinado servidor virtual;
- 3.1.138. Deve possuir capacidade de importação dos certificados e chaves criptográficas, para transações seguras entre cliente/servidor, podendo assim operar em modo “man in the middle”, ou seja, descriptografar, otimizar e re-criptografar o tráfego SSL/TLS sem comprometer a segurança da conexão SSL estabelecida previamente entre cliente/servidor.
- 3.1.139. Possuir recursos para configurar o equipamento para recriptografar em SSL a requisição ao enviar para

o servidor, permitindo as demais otimizações em ambiente 100% criptografado

3.1.140. A solução deve possuir diversos recursos relacionados ao uso de criptografia com o objetivo de otimizar e minimizar o impacto na performance das aplicações. Dentre eles deve ser possível configurar parâmetros como:

3.1.140.1. SSL session cache Timeout;

3.1.140.2. Session Ticket;

3.1.140.3. OCSP (Online Certificate Status Protocol) Stapling;

3.1.140.4. Dynamic Record Sizing;

3.1.140.5. ALPN (Application Layer Protocol Negotiation);

3.1.140.6. Perfect Forward Secrecy;

3.1.141. Todas as funcionalidades de inspeção, proteção e aceleração de tráfego criptografado através de SSL/TLS especificadas neste edital devem estar disponíveis quando a conexão segura for estabelecida usando:

3.1.141.1. Autenticação do servidor por parte do cliente, através da verificação da validade do certificado digital fornecido pelo lado servidor durante o processo de estabelecimento do túnel SSL/TLS;

3.1.141.2. Autenticação do cliente por parte do servidor, através da solicitação e verificação da validade do certificado digital fornecido pelo cliente durante o processo de estabelecimento do túnel SSL/TLS;

3.1.141.3. Ambas as autenticações acima mencionadas ocorrendo de forma simultânea;

3.1.141.4. Ao realizar inspeção, proteção, OffLoad e aceleração de tráfego criptografado através de SSL/TLS;

3.1.141.5. Encaminhar ao servidor real via cabeçalho HTTP ou de forma transparente, todo o certificado digital utilizado pelo lado cliente para se autenticar perante o servidor durante o processo de estabelecimento do túnel SSL/TLS.

3.1.142. Deve possibilitar a customização da interface gráfica da página de login.

3.1.142. A solução deve oferecer ferramenta de Portal de Acesso de Usuários que permita que usuários acessem aplicações internas a partir de rede externas, implementando as funcionalidades de Single Sign-on e/ou VPN-SSL, com, pelo menos, os seguintes recursos para cada funcionalidade:

3.1.142.1. Single Sign-on:

3.1.142.1.a) modo “Portal” onde o equipamento se comporta como proxy reverso, buscando o conteúdo Web dos portais internos e apresentando-os como links seguros no portal do usuário;

3.1.142.1.b) Ser capaz de solicitar as credenciais do usuário somente uma vez, e autenticar o usuário em todos os portais que requeiram autenticação, fazendo cache das credenciais do usuário e utilizar a credencial correta para cada sistema.

3.1.142.2. VPN-SSL:

3.1.142.2.a) modo “Túnel por aplicação” onde o usuário estabelece túnel somente para o tráfego da aplicação, não sendo permitido outro tipo de tráfego dentro do mesmo túnel;

3.1.142.2.b) modo “Portal” onde o equipamento se comporta como proxy reverso, buscando o conteúdo Web dos portais internos e apresentando-os como links seguros no portal do usuário;

3.1.142.2.c) modo “Network”, onde um usuário se conecta efetivamente à rede interna, obtendo um endereço IP roteável pela rede interna;

3.1.142.2.d) Ser capaz de solicitar as credenciais do usuário somente uma vez, e autenticar o usuário em todos os portais que requeiram autenticação, fazendo cache das credenciais do usuário e utilizar a credencial correta para cada sistema.

3.1.142.2. e) Deverá ser compatível para Microsoft Windows, Linux, dispositivos/ baseados em Android e iOS e MAC OSX;

3.1.143. Para a ferramenta de Portal de Acesso de Usuários, deverá ser capaz de autenticar usuários em bases de dados, como por exemplo: LDAP, Radius, Tacacs+, Kerberos e RSA SecurID;

3.1.144. Deve suportar autenticação de múltiplos fatores utilizando tokens de Hardware ou one-time passcode (OTP); Deve possuir capacidade para realizar proxy reverso com a finalidade de omitir a URI real, promovendo assim o acesso seguro as aplicações web internas;

3.1.145. Melhora da disponibilidade das aplicações através do balanceamento da entrada de tráfego deve possuir, ao menos, as seguintes características:

3.1.145.1. DNS autoritativo;

3.1.145.2. DNS secundário;

3.1.145.3. DNS resolver;

3.1.145.4. DNS cache;

3.1.145.5. Balanceamento de DNS servers;

3.1.145.6. DNSSec;

3.1.146. Capacidade de uso de chave criptográfica TSIG para comunicação segura entre servidores DNS, obedecendo no mínimo os padrões: HMAC MD5, HMAC SHA-1 ou HMAC SHA-256;

3.1.147. A solução deve realizar o offload dos servidores de DNS, funcionando como o DNS secundário;

3.1.148. A solução deve suportar pelo menos os seguintes tipos de requisição DNS: SOA, A, AAAA, CNAME, DNAME, HINFO, MX, NS, PTR, SRV, TXT

3.1.149. Deve ser capaz de gerar estatísticas sobre consultas de DNS por: Aplicação, nome da query, tipo da

query, endereço IP do cliente;

3.1.150. Deve ser possível configurar a solução de modo inline a estrutura de DNS existente e transparente sem requerer grandes mudanças na infraestrutura;

3.1.151. Deve prover as respostas a queries DNS da própria RAM CACHE

3.1.152. A solução deve ser capaz de realizar IP Anycast;

3.1.153. A solução deve ser capaz de realizar DNSSEC, independente da estrutura dos servidores DNS em uso

3.1.154. A solução de alta disponibilidade não deve depender de BGP ou outro protocolo de roteamento;

3.1.155. A solução deve suportar, no mínimo, os seguintes métodos de balanceamento:

3.1.155.1. Round Robin;

3.1.155.2. Global Availability;

3.1.155.3. Geografia;

3.1.155.4. Least Connections;

3.1.156. A solução deve ser capaz de lidar com clientes IPv6 quando o site atende apenas com IPv4 (requests AAAA ou A6);

3.1.157. A solução deve suportar edns-client-subnet (ECS) para tanto responder requisições de clientes ou encaminhar requisições de clientes (screening).

3.1.158. Baseado no ECS DNS deve ser possível preservar o endereço IP da subnet do cliente ao invés do LDNS para tomar decisões .

3.1.159. A solução deve funcionar pelo menos das seguintes formas:

3.1.159.1. Usar o ECS para tomar decisões baseado em topologia (Subnets)

3.1.159.2. Injetar o ECS (proxy requests) para outros servidores DNS

3.1.160. A solução deve fazer persistência baseado no endereço IP do cliente (ECS), significando que se o cliente mudar de LDNS resolver (suporte ECS).

3.1.161. Possuir recursos para executar compressão de conteúdo HTTP, para reduzir a quantidade de informações enviadas ao cliente;

3.1.162. Possuir no mínimo um dos tipo de compressão a seguir: gzip1 a gzip9 ou deflate;

3.1.163. Possuir capacidade para definir compressão especificamente para certos tipos de objetos;

3.1.164. Permitir o balanceamento de aplicações em um pool de servidores, independentemente do hardware, sistema operacional e tipo de aplicação;

3.1.165. A solução deve permitir aplicar criptografia de cookies para a proteção dos cookies utilizados pela aplicação web.

3.1.166. Possuir recursos para balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência de sessão dos seguintes tipos:

3.1.166.1. Por cookie;

3.1.166.2. Endereço de origem;

3.1.166.3. Sessão SSL;

3.1.166.4. Análise da URL acessada;

3.1.166.5. Através de qualquer parâmetro do cabeçalho HTTP;

3.1.166.6. MS Terminal Services Session (MSRDP);

3.1.166.7. Através da análise do SIP Call ID ou Source IP;

3.1.166.8. Através da análise de qualquer informação da porção de dados (camada 7);

3.1.167. O equipamento oferecido deverá suportar os seguintes métodos de monitoramento dos servidores reais:

3.1.167.1. ICMP, TCP, HTTP, HTTPS;

3.1.167.2. Devem existir monitores predefinidos para, no mínimo, os seguintes protocolos: ICMP, HTTP, HTTPS, Diameter, FTP, SASP, SMB, RADIUS, MSSQL, NNTP, ORACLE, RPC, LDAP, IMAP, SMTP, POP3, SIP, Real Server, SOAP, SNMP e WMI;

3.1.168. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor;

3.1.169. Realizar Network Address Translation (NAT);

3.1.170. Realizar proteção contra syn flood;

3.1.171. Realizar as proteções de cabeçalho: X-Frame-Options, X-XSS-Protection, X-Content-Type-Options

3.1.172. Permitir espelhamento do tráfego, de forma que a solução envie uma cópia do tráfego para um analisador, como por exemplo um pool de IDSs ou Sniffers, para fins de análise de tráfego de rede ou mesmo para identificação de padrões de acesso não permitidos ou indicações de atividade maliciosas ou ataques de rede;

3.1.173. A solução deve possuir recurso de ativação de grupo prioritário, no qual o administrador pode especificar a quantidade mínima de servidores que devem estar disponíveis em cada grupo e a prioridade dos grupos.

3.1.173.1. Caso o número de servidores disponíveis fique menor do que o estipulado pelo administrador, a solução deve automaticamente distribuir o tráfego para o próximo grupo com maior prioridade não afetando o serviço.

3.1.173.2. Caso o número de servidores disponíveis volte ao valor mínimo estipulado pelo administrador, a solução deve automaticamente retirar o grupo com menor prioridade de balanceamento, voltando ao estado original.

3.1.174. Possuir capacidade de abrir um número reduzido de conexões TCP com o servidor e inserir os HTTP

requests gerado pelos clientes nestas conexões, reduzindo a necessidade de estabelecimento de conexões nos servidores e aumentando a performance do serviço

- 3.1.175. A solução deve possuir solução de Cache em memória Ram;
- 3.1.176. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor real;
- 3.1.177. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor virtual;
- 3.1.178. Possuir recursos para limitar o número de sessões estabelecidas com cada grupo de servidores;
- 3.1.179. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor físico;
- 3.1.180. Realizar Network Address Translation (NAT);
- 3.1.181. Realizar Proteção contra Denial of Service (DoS);
- 3.1.182. Realizar Proteção contra Syn flood;
- 3.1.183. Realizar Limpeza de cabeçalho HTTP;
- 3.1.184. Deve possuir suporte a Link Layer Discovery Protocol (LLDP);
- 3.1.185. Suporte a otimização do protocolo TCP para ajustes a parâmetros das conexões clientes e servidor;
- 3.1.186. Deve ser capaz de realizar DHCP relay;
- 3.1.187. Deve possuir relatórios das aplicações, com pelos menos os seguintes gráficos:
 - 3.1.187.1. Tempo de resposta da aplicação;
 - 3.1.187.2. Latência;
 - 3.1.187.3. Conexões para conjunto de servidores, servidores individuais;
 - 3.1.187.4. Por URL;
 - 3.1.187.5. A solução deve ter suporte a TLS 1.3.

ITEM	DESCRIÇÃO	UNIDADE DE MEDIDA	QUANT
2	FORNECIMENTO DE SOLUÇÃO DE WEB APPLICATION FIREWALL(WAF), DO TIPO APPLIANCE FÍSICO, COM GARANTIA DE 60(SESENTA) MESES.	UN	20

3.2. Especificação técnica mínima

- 3.2.1. Os appliances físicos devem ser novos e de primeiro uso;
- 3.2.2. Os equipamentos devem ser fornecidos em modo appliance, com conjunto de hardware e software dedicados, não podendo ser servidor de uso genérico, e que atendam todas as funcionalidades descritas neste Termo de Referência.
- 3.2.3. Devem ser novos, sem uso prévio e entregues em perfeito estado de funcionamento. Não devem ser remanufaturados, reconicionados ou possuir reparos de qualquer espécie.
- 3.2.4. Não serão aceitos equipamentos ou softwares que constem em anúncio ou lista do tipo end-of-sale, end-of-support ou end-of-life do fabricante, ou seja, produtos que serão descontinuados, perderão suporte e garantia oficiais do fabricante.
- 3.2.5. O equipamento deve se instalar em rack com largura padrão de 19 polegadas, padrão EIA-310, ocupando no máximo 2Us do referido rack;
- 3.2.6. Deverão ser fornecidos todos os cabos, suportes (se necessários, "gavetas", "braços" e "trilhos"), incluindo todos os cabos de ligação lógica e elétrica necessários à instalação e perfeito funcionamento do equipamento no rack;
- 3.2.7. Deve ser fornecido com todos os cabos de ligação lógica e elétrica necessários à instalação e perfeito funcionamento.
- 3.2.8. Dispor de fonte de alimentação redundante com tensão de entrada de 110V a 220V AC automática e frequência de 60Hz;
- 3.2.9. Possuir sistema operacional customizado especificamente para funções de Web Application Firewall, não podendo ser entregue appliance do tipo NGFW;
- 3.2.10. Possuir, no mínimo, 06 interfaces, sendo 02 de 10GE com conectores padrão SFP+ (SR) e 04 portas SFP e transceivers (SR ou UTP); Serão aceitas interfaces de maior capacidade, desde que possibilitem ser transformados em 10 GE (incluindo os cabos "breakout" de no mínimo 3 metros);
- 3.2.11. Possuir 01 interfaces 1GE, incluso interfaces de gerência com conectores padrão RJ45;
- 3.2.12. Todas as interfaces fornecidas devem estar licenciadas e habilitadas para uso imediato;
- 3.2.13. Possuir no mínimo de 8.000 Mbps de throughput em camada 7;
- 3.2.14. Possuir capacidade de 4.000 transações por segundo (TPS) em TLS padrão RSA (chaves de 2.048 bit);
- 3.2.15. Possuir no mínimo compressão em hardware de 5.000 Mbps em (tráfego HTTP/HTTPS);
- 3.2.16. Recursos de agregação de portas baseado no protocolo LACP, segundo o padrão IEEE 802.3ad;
- 3.2.17. Memória RAM mínima de 16 GB;
- 3.2.18. Disco rígido com capacidade de armazenamento interno e retenção de logs para análise com capacidade

mínima de 240GB;

3.2.19. Deve vir acompanhado de todas as licenças de software ou hardware necessárias para atendimento das funcionalidades exigidas neste caderno de especificações técnicas;

3.2.20. Todas as funcionalidades devem continuar ativas, mesmo após o término do termo de garantia e suporte técnico.

3.2.21. Garantir que na aceleração de SSL, tanto a troca de chaves quanto a criptografia dos dados seja realizada com aceleração em hardware, para não onerar o sistema

3.2.22. Suportar e garantir a instalação em ambiente de alta disponibilidade;

3.2.23. Deve permitir a configuração da solução em alta disponibilidade, permitindo o funcionamento em cluster do tipo ativo-passivo e ativo-ativo.

3.2.24. A solução deve suportar mais do que dois elementos no cluster para sincronização de configuração de forma nativa a fim de permitir escalabilidade no futuro.

3.2.25. Implementar a sincronização entre os equipamentos redundantes, assegurando que não haverá "downtime" e queda de sessões em caso de falha de uma das unidades.

3.2.26. Deve possuir redundância de dispositivos, de maneira que, em caso de falha de um dos equipamentos, o estado de todas as conexões seja remanejado para o equipamento redundante, preservando o estado original de todas as tabelas de conexões e de persistência.

3.2.27. O equipamento deve permitir a sincronização das configurações de forma automática.

3.2.28. Caso seja necessária uma interligação entre os equipamentos, a CONTRATADA será integralmente responsável por tal interligação, garantindo a performance necessária para o atendimento da solução.

3.2.29. O equipamento, quando habilitado para mais de uma função (Balanceamento, DNS, Web Application Firewall, etc), deverá permitir a definição da importância da função para cada tipo de funcionalidade;

3.2.30. Possuir capacidade para gerenciar os recursos disponíveis de acordo com as funções habilitadas nos equipamentos SLB, GSLB, WAF, etc.

3.2.31. Fornecer recurso para o transporte de múltiplas VLANs por uma única porta (ou por um conjunto agregado de portas) utilizando o protocolo 802.1q;

3.2.32. Analisar e proteger tráfego HTTP/1.0, HTTP/1.1, HTTP/2.0 e/ou HTTP/3;

3.2.33. Possuir suporte a IPv6;

3.2.34. A solução deve permitir o encapsulamento, em camada 3, do tráfego entre o balanceador e o servidor para tráfego IPv4 e IPv6, quando o balanceamento é realizado apenas em direção ao servidor, onde a resposta do servidor real é enviada diretamente ao cliente;

3.2.35. Deve suportar, no mínimo, 1000 VLANs simultaneamente;

3.2.36. Implementar o SNTP (Simple Network Time Protocol) ou NTP (Network Time Protocol);

3.2.37. Possuir suporte à funcionalidade de VXLAN, essencial para integração com o ambiente de virtualização (Software Defined Network).

3.2.38. Assinar cookies digitalmente e editar endereços de URL ("URL Rewriting");

3.2.39. O equipamento deverá permitir a sincronização das configurações:

3.2.39.1.1. De forma automática;

3.2.39.1.2. Manualmente, forçando a sincronização apenas no momento desejado;

3.2.40. Permitir a configuração das interfaces de alta disponibilidade do cluster (heartbeat), com opções para:

3.2.40.1.1. Compartilhar a rede de heartbeat com a rede de dados;

3.2.40.1.2. Utilizar uma rede exclusiva para o heartbeat.

3.2.41. Permitir que regras customizadas em linguagem aberta possam ser utilizadas para customizar a distribuição dinâmica de tráfego e aumentar a proteção contra ataques;

3.2.42. A solução deve possuir linguagem de programação open-source que permita a manipulação do tráfego de entrada e saída, viabilizando assim a alteração de parâmetros no cabeçalho e no corpo das mensagens.

3.2.43. Essa linguagem de programação deve permitir a importação de pacotes, garantindo assim que a agilidade e flexibilidade no compartilhamento dos scripts.

3.2.44. Permitir a criação de políticas através de interface gráfica web para manipulação de tráfego através de lógica para pelo menos os seguintes operadores:

3.2.45. GEOIP, http-basic-auth, http-cookie, http-header, http-host, http-method, http-referer, http-set-cookie, http-status, http-uri e http-version

3.2.46. A solução deve possuir políticas de uso de senhas administrativas tais como: nível de complexidade, período de validade e travamento de conta devido a erros múltiplos de login de forma nativa ou no mínimo integrado a uma base Active Directory ou LDAP ou tacacs;

3.2.47. Deve implementar configuração de endereçamento IP estático ou dinâmico (DHCP/BOOTP) para a interface de gerenciamento

3.2.48. Permitir acesso in-band via SSH

3.2.49. Possuir console de administração com interface gráfica remota segura atendendo os seguintes requisitos:

3.2.49.1. Permitir a definição de diferentes níveis de administração, no mínimo, um nível completo e outro somente de visualização de configurações e logs;

3.2.49.2. Permitir a replicação de configurações e a aplicação de atualização de softwares para os elementos dos nós do cluster;

3.2.50. Manter internamente múltiplos arquivos de configurações do sistema;

3.2.51. Utilizar SCP ou HTTPS como mecanismo de transferência de arquivos de configuração e Sistema

Operacional;

3.2.52. Os usuários de gerência deverão poder ser autenticados em bases remotas. No mínimo RADIUS, LDAP e TACACS+ deverão ser suportados;

3.2.53. Deverá ser possível associar aos usuários de bases externas como RADIUS, LDAP e TACACS+ o nível de acesso;

3.2.54. Possuir Interface Gráfica via Web;

3.2.55. Possuir auto-complementação de comandos na CLI;

3.2.56. Possuir ajuda contextual;

3.2.57. A Solução deve ter a capacidade de permitir a criação de MIBs customizadas ou ter suporte a snmpv1/v2/v3 para monitoramento do equipamento;

3.2.57.1. A solução deve possuir arquivo de MIBs e documento descrevendo os OIDs e o que é possível coletar utilizando SNMP;

3.2.58. A Solução deve ter suporte a sFlow;

3.2.59. Interface por linha de comando (CLI – Command Line Interface) que possibilite a configuração dos equipamentos;

3.2.60. Possuir, no mínimo, Três níveis de usuários na GUI – Super-Usuário, Usuário com permissões reduzidas, e usuário Somente Leitura;

3.2.61. A interface Gráfica deverá permitir a atualização do sistema operacional e/ou a instalação de patches ou Hotfixes sem o uso da linha de comando;

3.2.62. A interface gráfica deverá permitir a configuração de qual partição o equipamento deverá dar o boot;

3.2.63. Possuir um comando, via CLI, que mostre o tráfego de utilização das interfaces (bps e pps);

3.2.64. Suportar a rollback de configuração e imagem;

3.2.65. Possuir e fornecer geração de mensagens de syslog para eventos relevantes ao sistema;

3.2.66. Possuir configuração de múltiplos syslog servers para os quais o equipamento irá enviar as mensagens de syslog;

3.2.67. Possuir armazenamento de mensagens de syslog em dispositivo interno ao equipamento;

3.2.68. A interface Gráfica deverá permitir a reinicialização do equipamento;

3.2.69. Reinicialização do equipamento por comando na CLI;

3.2.70. Possuir recurso de gerência via SNMP e implementar SNMPv1, SNMPv2c e SNMPV3;

3.2.71. Possuir traps SNMP;

3.2.72. Caso a solução possua suporte a RMON, deverá possuir suporte a monitoração utilizando pelo menos 4 grupos: statistics, history, alarms e events.

3.2.73. Os logs de sistema devem ter a opção de ser armazenados internamente ao sistema ou em servidor externo;

3.2.74. Implementar Debugging: CLI via console e SSH;

3.2.75. Permite a criação de políticas diferenciadas por aplicação e por URL, onde cada aplicação e URL poderão ter políticas totalmente diferentes;

3.2.76. Permitir a criação de políticas diferenciadas por aplicação.

3.2.77. Deverá possuir uma funcionalidade de criação automática de políticas, onde a política de segurança é criada e atualizada automaticamente baseando-se no tráfego real observado à aplicação;

3.2.78. O perfil aprendido de forma automatizada pode ser ajustado, editado ou bloqueado;

3.2.79. Restringir métodos HTTP/ HTTPS permitidos, tipos ou versões de protocolos, tipos de caracteres e versões utilizadas de cookies;

3.2.80. Permitir as seguintes opções de implementação:

3.2.81. Monitoramento (sem bloqueio);

3.2.82. Proxy (reverso e transparente).

3.2.83. Permitir que novas políticas fiquem apenas monitorando o tráfego, sem bloqueá-lo, indicando caso aconteça algum evento;

3.2.84. Remover as mensagens de erro do conteúdo que será enviado aos usuários;

3.2.85. Em modo “monitoramento” (sem bloqueio), realizar análise e avaliação do tráfego, gerar relatórios com os dados analisados e simular bloqueios para efeito de avaliação;

3.2.86. Proteger contra-ataques automatizados, incluindo bots e web scraping, identificando comportamento não humano, navegadores operados por scripts ou qualquer outra forma que não operados por humanos;

3.2.87. Bloquear ataques aos servidores de aplicação, por meio dos seguintes recursos:

3.2.87.1. Identificação, isolamento e bloqueio de ataques sofisticados sem impactar nas transações das aplicações;

3.2.87. Possuir firewall XML integrado com suporte a filtro e validação de funções XML específicas da aplicação;

3.2.88. A solução deve suportar e fazer a proteção do tráfego de protocolo WebSocket.

3.2.89. Com a finalidade de proteger as aplicações, a solução deve suportar o uso de páginas de login AJAX/JSON tanto com configuração manual como descoberta automática.

3.2.90. Permitir a utilização de modelo positivo de segurança para proteger contra ataques às aplicações HTTP e HTTPS, além de proteção contra- ataques conhecidos aos protocolos HTTP e HTTPS;

3.2.91. Quando detectada uma tentativa de ataque bloquear de imediato o tráfego ou a sessão;

3.2.92. Bloqueio com intermediação e interrupção da conexão;

- 3.2.93. Criação de políticas automáticas que bloqueiam o endereço IP que realizar violações;
- 3.2.94. Utilização de página HTML informativa e personalizável como HTTP Response aos bloqueios;
- 3.2.95. Configuração de políticas de bloqueio baseadas em requisição HTTP, endereço IP e usuário de aplicação;
- 3.2.96. Permitir apenas transações de aplicações validadas, o restante das transações deverá ser bloqueado, utilizando bloqueio por nível de aplicação baseado no contexto da sessão do usuário, com privilégios de autorização diferentes, entradas de usuários e tempo de resposta de aplicação;
- 3.2.97. Identificar e armazenar o ataque acontecido com detalhes, com as seguintes informações:
 - 3.2.97.1. Endereços IP que originaram os ataques;
 - 3.2.97.2. Horário do ataque;
 - 3.2.97.3. Nome do ataque;
 - 3.2.97.4. Qual campo foi atacado;
 - 3.2.97.5. Quantas vezes esse ataque foi realizado;
- 3.2.98. Possuir mecanismo de aprendizado automatizado capaz de identificar todos os conteúdos das aplicações, incluindo URLs, parâmetros URLs, campos de formulários, o que se espera de cada campo (tipo de dado, tamanho de caracteres, se é um campo obrigatório), cookies, ações SOAP e elementos XML; identificar e criar perfil de utilização dos aplicativos, inclusive desenvolvidos em Javascript, CGI, ASP e PHP;
- 3.2.99. O perfil aprendido de forma automatizada pode ser ajustado, editado ou bloqueado;
- 3.2.100. Identificar ataques baseados em:
 - 3.2.100.1. Assinaturas, com atualização periódica da base pelo fabricante;
 - 3.2.100.2. Regras;
 - 3.2.100.3. Perfis de utilização;
- 3.2.101. Deve possuir tecnologia para mitigação de DDoS em camada 7 baseado em análise comportamental, usando o aprendizado.
- 3.2.102. Não deve haver a necessidade de intervenção de usuário para configurar thresholds DoS pois esses valores devem ser auto-ajustáveis e adaptativos de acordo com mudanças.
- 3.2.103. A solução deve possuir a capacidade de automaticamente capturar tráfego no formato TCP Dump relativos a ataques DoS L7, Web Scraping e força bruta permitindo uma análise mais aprofundada por parte do administrador.
- 3.2.104. Detectar ataques de força bruta por meio dos seguintes métodos:
- 3.2.105. Aumento do tempo de resposta da aplicação monitorada ou bloqueio temporário do atacante;
- 3.2.106. Quantidade de transações por segundo (TPS), monitorando a quantidade de transações por segundo por endereço IP.
- 3.2.107. Detectar ataques do tipo força bruta em que:
 - 3.2.107.1. O atacante solicita repetidamente o mesmo recurso;
 - 3.2.107.2. O atacante realiza repetidas tentativas não autorizadas de acesso;
 - 3.2.107.3. São utilizados ataques automatizados de login.
- 3.2.108. Detectar ataques do tipo força bruta que explorem:
 - 3.2.108.1. Controles de acesso da aplicação (Erro 401 – Unauthorized);
 - 3.2.108.2. Solicitações repetidas ao mesmo recurso, em qualquer parte/URL da aplicação;
 - 3.2.108.3. Aplicações WEB que não retornam o erro 401 por meio da identificação de expressão regular no retorno/página de erro da aplicação);
 - 3.2.108.4. Gerenciamento de sessão (muitas sessões de um único endereço IP ou a um range de Ips);
 - 3.2.108.5. Clientes automatizados (robôs, requisições muito rápidas);
 - 3.2.108.6. Permitir a criação de políticas diferenciadas por aplicação e por URL, onde cada aplicação e URL poderão ter políticas totalmente diferentes;
 - 3.2.108.7. Possuir mecanismo para criação dinâmica de política de segurança, com aprendizado automático de padrão de utilização da aplicação, realizado sobre o fluxo de tráfego bidirecional atravessando o equipamento;
 - 3.2.108.8. Possibilitar atualização de novas assinaturas para ataques conhecidos;
- 3.2.109. Apresentar proteção contra-ataques, como:
 - 3.2.109.1. Brute Force Login;
 - 3.2.109.2. Buffer Overflow;
 - 3.2.109.3. Cookie Injection;
 - 3.2.109.4. Cookie Poisoning;
 - 3.2.109.5. Cross Site Request Forgery (CSRF);
 - 3.2.109.6. Cross Site Scripting (XSS);
 - 3.2.109.7. Server Side Request Forgery (SSRF)
 - 3.2.109.8. Directory Traversal;
 - 3.2.109.9. Forceful Browsing;
 - 3.2.109.10. HTTP Denial of Service;
 - 3.2.109.11. HTTP hidden field manipulation;
 - 3.2.109.12. HTTP request smuggling;
 - 3.2.109.13. HTTP Response Splitting;
 - 3.2.109.14. Malicious Robots;
 - 3.2.109.15. Parameter Tampering;

- 3.2.109.16. Remote File Inclusion Attacks;
- 3.2.109.17. Sensitive Data Leakage (Social Security Numbers, Cardholder Data, PII, HPI);
- 3.2.109.18. Session Hijacking;
- 3.2.109.19. SQL Injection;
- 3.2.109.20. Web Scraping;
- 3.2.109.21. Web server software and operating system attacks;
- 3.2.109.22. Web Services (XML) attacks;
- 3.2.110. Permitir configurar granularmente, por aplicação protegida, restrições de métodos HTTP permitidos, tipos ou versões de protocolos, tipos de caracteres e versões utilizadas de cookies;
- 3.2.111. Suportar os seguintes critérios de decisão para realizar bloqueio ou gerar alerta, sendo que uma política pode conter um ou mais critérios simultaneamente:
 - 3.2.111.1. Assinatura de ataque ou Ips de atacantes conhecidos;
 - 3.2.111.2. Código de response;
 - 3.2.111.3. Conteúdo da cookie;
 - 3.2.111.4. Conteúdo do cabeçalho;
 - 3.2.111.5. Conteúdo do payload;
 - 3.2.111.6. Hostname;
 - 3.2.111.7. IP de origem;
 - 3.2.111.8. Método HTTP;
 - 3.2.111.9. Número de ocorrências em determinado intervalo de tempo;
 - 3.2.111.10. Parâmetro;
 - 3.2.111.11. User-agent (navegador);
- 3.2.112. Deve proteger contra os seguintes ataque por meio de assinaturas seletivas:
 - 3.2.112.1. Ataques de negação de serviços automatizados;
 - 3.2.112.2. Worms e vulnerabilidades conhecidas;
 - 3.2.112.3. Requests em objetos restritos;
- 3.2.113. Deve proteger contra ataques SSRF (Server Side RequestForgery);
- 3.2.114. A solução oferecida deverá possuir proteção contra ataques, disponibilizando acesso a base de assinaturas e atualizações periódicas ate o fim do contrato;
- 3.2.115. Ao atualizar ou adicionar uma nova assinatura, a solução deve automaticamente colocar essa assinatura em modo “staging” para evitar falsos positivos e não bloquear tráfego válido. Depois de um período a mesma deve automaticamente entrar em modo de bloqueio.
- 3.2.116. Deve permitir que possa ser especificado na política os tipos de arquivos que serão bloqueados (File Types);
- 3.2.117. A solução deve permitir a inspeção de upload de arquivos para os servidores de aplicação, ou enviar para inspeção através do protocolo ICAP;
- 3.2.118. Deve possuir uma proteção proativa comportamental contra ataques automatizados por robôs e outras ferramentas de ataque;
- 3.2.119. Ao detectar uma condição de DDoS, assinaturas dinâmicas devem ser automaticamente criadas e implementadas em tempo real para proteção da aplicação;
- 3.2.120. A solução deve possuir proteção de DDoS L7 baseado em análise comportamental, sem precisar de nenhuma configuração manual;
- 3.2.121. Possuir método de mitigação de DoS L7 baseado em:
 - 3.2.121.1. Descarte de todas as requisições de um determinado IP e/ou país suspeito;
 - 3.2.121.2. CAPTCHA para suspeitos que ultrapassarem os thresholds;
 - 3.2.121.3. Defesa proativa contra Bot, através da injeção de um desafio no Browser ou via Javascript para detectar se é um usuário legítimo ou robô;
- 3.2.122. Deve aprender automaticamente o comportamento da aplicação e combinar o comportamento heurístico do tráfego, análise de dados e Machine Learning, com o stress do servidor de aplicação para determinar uma condição de DDoS;
- 3.2.123. Aprender o comportamento da aplicação:
 - 3.2.123.1. Campos, valores, cookies e URLs;
- 3.2.124. Políticas sugeridas somente devem ser aplicadas após um período configurável;
- 3.2.125. Inspeccionar e monitorar até a camada de aplicação, todo tráfego de dados HTTP, incluindo cabeçalhos, campos de formulários e conteúdo, além de inspecionar os requests e responses;
- 3.2.126. Realizar as checagens em todos os tipos de entrada de dados, como URLs, formulários, cookies, campos ocultos e parâmetros, consultas (query), métodos HTTP, elementos XML e ações SOAP;
- 3.2.127. Proteger contra mensagens XML e SOAP malformadas;
- 3.2.128. Utilizar o campo HTTP X-Forwarded-For sem modificar seu conteúdo de origem, permitindo a diferenciação em ambientes com NAT;
- 3.2.129. Remover as mensagens de erro do conteúdo que será enviado aos usuários;
- 3.2.130. Deverá permitir o bloqueio de robôs (bots) que acessam a aplicação através de detecção automática ou vir com lista dos principais robôs já pré configurada, inclusive para Robôs conhecidos do mercado, como por exemplo Google, Yahoo e Microsoft Bing, que deverão ser liberados por padrão.

- 3.2.131. Deverá permitir o cadastro de robôs que podem acessar a aplicação;
- 3.2.132. Deverá implementar proteção ao JSON (JavaScript Object Notation);
- 3.2.133. Implementar a segurança de web services, através dos seguintes métodos:
 - 3.2.133.1. Criptografar/Decriptografar partes das mensagens SOAP;
 - 3.2.133.2. Assinar digitalmente partes das mensagens SOAP;
 - 3.2.133.3. Verificação de partes das mensagens SOAP;
- 3.2.134. Deverá permitir o bloqueio de ataques de força bruta de usuário/senha em páginas de acesso (login) que protegem áreas restritas. Este bloqueio deve limitar o número máximo de tentativas e o tempo do bloqueio deverá ser configurável;
- 3.2.135. Deve encriptar dados e credenciais na camada de aplicação, sem ter a necessidade de atualizar a aplicação. Essas informações devem ser encriptadas para proteger o login e as credenciais dos usuários e com isso os dados da aplicação;
- 3.2.136. Deve proteger informações sensíveis e confidenciais da interceptação por terceiros, através da criptografia de dados quando ainda no browser do usuário. Deve proteger esses dados criptografados de malwares e keyloggers;
- 3.2.137. Deve ofuscar o nome de um parâmetro sensível da aplicação em caracteres randômicos. Esse nome de parâmetro deve ser mudado constantemente pela ferramenta para dificultar ataques direcionados;
- 3.2.138. Deverá possuir controle de fluxo por aplicação permitindo definir o fluxo de acesso de uma URL para outra da mesma aplicação. Dessa forma qualquer tentativa de acesso a um determinado site que não siga o fluxo passando pelas URLs pré-definidas deverá ser bloqueado como uma tentativa de acesso ilegal;
- 3.2.139. A solução deverá se integrar a soluções de análise (Scanner) de terceiros, de forma automática ou manual, como por exemplo Trustwave App Scanner (Cenzic), White Hat Sentinel, IBM AppScan, Qualys, QuotiumSeeker, HP Webinspect, Tenable; com a capacidade de criar regras para proteção das vulnerabilidades encontradas na análise do Scanner.
- 3.2.140. A solução deve fornecer relatórios consolidados de ataques com pelo menos os seguintes dados:
 - 3.2.140.1. Resumo geral com as políticas ativas, anomalias e estatísticas de tráfego, Ataques DoS, Ataques de Força Bruta, Ataques de Robôs, Violações, URL, Endereços IP, Países, Severidade.
- 3.2.141. Deverá permitir o agendamento de relatórios a serem entregues por email;
- 3.2.142. Emitir os seguintes relatórios gráficos dos alterar por:
 - 3.2.142.1. Política de segurança;
 - 3.2.142.2. Tipos de ataques;
 - 3.2.142.3. Violações;
 - 3.2.142.4. URL que foram atacadas;
 - 3.2.142.5. Endereços IP de origem;
 - 3.2.142.6. localização geográfica dos endereços IPs de origem;
 - 3.2.142.7. Severidade;
 - 3.2.142.8. Código de resposta;
 - 3.2.142.9. Métodos;
 - 3.2.142.10. Protocolos;
 - 3.2.142.11. Sessão;
- 3.2.143. Permitir a seleção de período para emissão dos relatórios,
- 3.2.144. Permitir a geração das seguintes informações, por período:
 - 3.2.144.1. Permitir auditoria detalhada das alterações de configuração efetuadas, indicando usuário, ação e horário;
 - 3.2.144.2. Informações estatísticas de quantidade de conexões completadas e bloqueadas;
 - 3.2.144.3. Informações estatísticas de fluxo de tráfego;
 - 3.2.144.4. Informações estatísticas de quantidade de sessões ou conexões;
- 3.2.145. Identificação, isolamento e bloqueio de ataques sofisticados para os protocolos: HTTP e HTTPS;
- 3.2.146. Deve possuir capacidade para definir que todo tráfego seja tunelado e permitir a utilização do protocolo padrão HTTPS com SSL como transporte, possibilitando a sua utilização com proxy HTTP e possibilitar utilização de encapsulamento
- 3.2.147. Deve possuir capacidade para definir servidor virtual em HTTPS com perfil cliente SSL/TLS padrão e redirecionar tráfego HTTP para HTTPS para um determinado servidor virtual;
- 3.2.148. Deve possuir capacidade de importação dos certificados e chaves criptográficas, para transações seguras entre cliente/servidor, podendo assim operar em modo “man in the middle”, ou seja, descriptografar, otimizar e re-criptografar o tráfego SSL/TLS sem comprometer a segurança da conexão SSL estabelecida previamente entre cliente/servidor.
- 3.2.149. Possuir recursos para configurar o equipamento para recriptografar em SSL a requisição ao enviar para o servidor, permitindo as demais otimizações em ambiente 100% criptografado
- 3.2.150. A solução deve possuir diversos recursos relacionados ao uso de criptografia com o objetivo de otimizar e minimizar o impacto na performance das aplicações. Dentre eles deve ser possível configurar parâmetros como:
 - 3.2.150.1. SSL session cache Timeout;
 - 3.2.150.2. Session Ticket;
 - 3.2.150.3. OCSP (Online Certificate Status Protocol) Stapling;

- 3.2.150.4. Dynamic Record Sizing;
- 3.2.150.5. ALPN (Application Layer Protocol Negotiation);
- 3.2.150.6. Perfect Forward Secrecy;
- 3.2.151. Todas as funcionalidades de inspeção, proteção e aceleração de tráfego criptografado através de SSL/TLS especificadas neste edital devem estar disponíveis quando a conexão segura for estabelecida usando:
 - 3.2.151.1. Autenticação do servidor por parte do cliente, através da verificação da validade do certificado digital fornecido pelo lado servidor durante o processo de estabelecimento do túnel SSL/TLS;
 - 3.2.151.2. Autenticação do cliente por parte do servidor, através da solicitação e verificação da validade do certificado digital fornecido pelo cliente durante o processo de estabelecimento do túnel SSL/TLS;
 - 3.2.151.3. Ambas as autenticações acima mencionadas ocorrendo de forma simultânea;
 - 3.2.151.4. Ao realizar inspeção, proteção, OffLoad e aceleração de tráfego criptografado através de SSL/TLS;
 - 3.2.151.5. Encaminhar ao servidor real via cabeçalho HTTP ou de forma transparente, todo o certificado digital utilizado pelo lado cliente para se autenticar perante o servidor durante o processo de estabelecimento do túnel SSL/TLS.
- 3.2.152. Deve possibilitar a customização da interface gráfica da página de login;
- 3.2.153. A solução deve oferecer ferramenta de Portal de Acesso de Usuários que permita que usuários acessem aplicações internas a partir de rede externas, implementando as funcionalidades de Single Sign-on e/ou VPN-SSL, com, pelo menos, os seguintes recursos para cada funcionalidade:
 - 3.2.153.1. Single Sign-on:
 - 3.2.153.1.a) modo “Portal” onde o equipamento se comporta como proxy reverso, buscando o conteúdo Web dos portais internos e apresentando-os como links seguros no portal do usuário;
 - 3.2.153.1.b) Ser capaz de solicitar as credenciais do usuário somente uma vez, e autenticar o usuário em todos os portais que requeiram autenticação, fazendo cache das credenciais do usuário e utilizar a credencial correta para cada sistema;
 - 3.2.153.2. VPN-SSL:
 - 3.2.153.2.a) modo “Túnel por aplicação” onde o usuário estabelece túnel somente para o tráfego da aplicação, não sendo permitido outro tipo de tráfego dentro do mesmo túnel;
 - 3.2.153.2.b) modo “Portal” onde o equipamento se comporta como proxy reverso, buscando o conteúdo Web dos portais internos e apresentando-os como links seguros no portal do usuário;
 - 3.2.153.2.c) modo “Network”, onde um usuário se conecta efetivamente à rede interna, obtendo um endereço IP roteável pela rede interna;
 - 3.2.153.2.d) Ser capaz de solicitar as credenciais do usuário somente uma vez, e autenticar o usuário em todos os portais que requeiram autenticação, fazendo cache das credenciais do usuário e utilizar a credencial correta para cada sistema;
 - 3.2.153.2.e) Deverá ser compatível para Microsoft Windows, Linux, dispositivos/ baseados em Android e iOS e MAC OSX;
- 3.2.153. Para a ferramenta de Portal de Acesso de Usuários, deverá ser capaz de autenticar usuários em bases de dados, como por exemplo: LDAP, Radius, Tacacs+, Kerberos e RSA SecurID;
- 3.2.154. Deve suportar autenticação de múltiplos fatores utilizando tokens de Hardware ou one-time passcode (OTP); Deve possuir capacidade para realizar proxy reverso com a finalidade de omitir a URI real, promovendo assim o acesso seguro as aplicações web internas;
- 3.2.155. Melhora da disponibilidade das aplicações através do balanceamento da entrada de tráfego deve possuir, ao menos, as seguintes características:
 - 3.2.155.1. DNS autoritativo;
 - 3.2.155.2. DNS secundário;
 - 3.2.155.3. DNS resolver;
 - 3.2.155.4. DNS cache;
 - 3.2.155.5. Balanceamento de DNS servers;
 - 3.2.155.6. DNSSec;
- 3.2.156. Capacidade de uso de chave criptográfica TSIG para comunicação segura entre servidores DNS, obedecendo no mínimo os padrões: HMAC MD5, HMAC SHA-1 ou HMAC SHA-256;
- 3.2.157. A solução deve realizar o offload dos servidores de DNS, funcionando como o DNS secundário;
- 3.2.158. A solução deve suportar pelo menos os seguintes tipos de requisição DNS: SOA, A, AAAA, CNAME, DNAME, HINFO, MX, NS, PTR, SRV, TXT
- 3.2.159 Deve ser capaz de gerar estatísticas sobre consultas de DNS por: Aplicação, nome da query, tipo da query, endereço IP do cliente;
- 3.2.160. Deve ser possível configurar a solução de modo inline a estrutura de DNS existente e transparente sem requerer grandes mudanças na infraestrutura;
- 3.2.161. Deve prover as respostas a queries DNS da própria RAM CACHE
- 3.2.162. A solução deve ser capaz de realizar IP Anycast;
- 3.2.163. A solução deve ser capaz de realizar DNSSec, independente da estrutura dos servidores DNS em uso
- 3.2.164. A solução de alta disponibilidade não deve depender de BGP ou outro protocolo de roteamento;

- 3.2.165. A solução deve suportar, no mínimo, os seguintes métodos de balanceamento:
- 3.2.165.1. Round Robin;
 - 3.2.165.2. Global Availability;
 - 3.2.165.3. Geografia;
 - 3.2.165.4. Least Connections;
- 3.2.166. A solução deve ser capaz de lidar com clientes IPv6 quando o site atende apenas com IPv4 (requests AAAA ou A6);
- 3.2.167. A solução deve suportar edns-client-subnet (ECS) para tanto responder requisições de clientes ou encaminhar requisições de clientes (screening).
- 3.2.168. Baseado no ECS DNS deve ser possível preservar o endereço IP da subnet do cliente ao invés do LDNS para tomar decisões .
- 3.2.169. A solução deve funcionar pelo menos das seguintes formas:
- 3.2.169.1. Usar o ECS para tomar decisões baseado em topologia (Subnets)
 - 3.2.169.2. Injetar o ECS (proxy requests) para outros servidores DNS
- 3.2.170. A solução deve fazer persistência baseado no endereço IP do cliente (ECS), significando que se o cliente mudar de LDNS resolver (suporte ECS).
- 3.2.171. Possuir recursos para executar compressão de conteúdo HTTP, para reduzir a quantidade de informações enviadas ao cliente;
- 3.2.172. Possuir no mínimo um dos tipo de compressão a seguir: gzip1 a gzip9 ou deflate;
- 3.2.173. Possuir capacidade para definir compressão especificamente para certos tipos de objetos;
- 3.2.174. Permitir o balanceamento de aplicações em um pool de servidores, independentemente do hardware, sistema operacional e tipo de aplicação;
- 3.2.175. A solução deve permitir aplicar criptografia de cookies para a proteção dos cookies utilizados pela aplicação web.
- 3.2.176. Possuir recursos para balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência de sessão dos seguintes tipos:
- 3.2.176.1. Por cookie;
 - 3.2.176.2. Endereço de origem;
 - 3.2.176.3. Sessão SSL;
 - 3.2.176.4. Análise da URL acessada;
 - 3.2.176.5. Através de qualquer parâmetro do cabeçalho HTTP;
 - 3.2.176.6. MS Terminal Services Session (MSRDP);
 - 3.2.176.7. Através da análise do SIP Call ID ou Source IP;
 - 3.2.176.8. Através da análise de qualquer informação da porção de dados (camada 7);
- 3.2.177. O equipamento oferecido deverá suportar os seguintes métodos de monitoramento dos servidores reais:
- 3.2.177.1. ICMP, TCP, HTTP, HTTPS;
 - 3.2.177.2. Devem existir monitores predefinidos para, no mínimo, os seguintes protocolos: ICMP, HTTP, HTTPS, Diameter, FTP, SASP, SMB, RADIUS, MSSQL, NNTP, ORACLE, RPC, LDAP, IMAP, SMTP, POP3, SIP, Real Server, SOAP, SNMP e WMI;
- 3.2.178. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor;
- 3.2.179. Realizar Network Address Translation (NAT);
- 3.2.180. Realizar proteção contra syn flood;
- 3.2.181. Realizar as proteções de cabeçalho: X-Frame-Options, X-XSS-Protection, X-Content-Type-Options
- 3.2.182. Permitir espelhamento do tráfego, de forma que a solução envie uma cópia do tráfego para um analisador, como por exemplo um pool de IDSs ou Sniffers, para fins de análise de tráfego de rede ou mesmo para identificação de padrões de acesso não permitidos ou indicações de atividade maliciosas ou ataques de rede;
- 3.2.183. A solução deve possuir recurso de ativação de grupo prioritário, no qual o administrador pode especificar a quantidade mínima de servidores que devem estar disponíveis em cada grupo e a prioridade dos grupos.
- 3.2.183.1. Caso o número de servidores disponíveis fique menor do que o estipulado pelo administrador, a solução deve automaticamente distribuir o tráfego para o próximo grupo com maior prioridade não afetando o serviço.
 - 3.2.183.2. Caso o número de servidores disponíveis volte ao valor mínimo estipulado pelo administrador, a solução deve automaticamente retirar o grupo com menor prioridade de balanceamento, voltando ao estado original.
- 3.2.184. Possuir capacidade de abrir um número reduzido de conexões TCP com o servidor e inserir os HTTP requests gerado pelos clientes nestas conexões, reduzindo a necessidade de estabelecimento de conexões nos servidores e aumentando a performance do serviço
- 3.2.185. A solução deve utilizar Cache Array Routing Protocol (CARP) no algoritmo de HASH;
- 3.2.186. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor real;
- 3.2.187. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor virtual;
- 3.2.188. Possuir recursos para limitar o número de sessões estabelecidas com cada grupo de servidores;
- 3.2.189. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor físico;
- 3.2.190. Realizar Network Address Translation (NAT);

- 3.2.191. Realizar Proteção contra Denial of Service (DoS);
 3.2.192. Realizar Proteção contra Syn flood;
 3.2.193. Realizar Limpeza de cabeçalho HTTP;
 3.2.194. Deve possuir suporte a Link Layer Discovery Protocol (LLDP);
 3.2.195. Suporte a otimização do protocolo TCP para ajustes a parâmetros das conexões clientes e servidor;
 3.2.196. Deve ser capaz de realizar DHCP relay;
 3.2.197. Deve possuir relatórios das aplicações, com pelos menos os seguintes gráficos:
 3.2.197.1. Tempo de resposta da aplicação;
 3.2.197.2. Latência;
 3.2.197.3. Conexões para conjunto de servidores, servidores individuais;
 3.2.197.4. Por URL;
 3.2.197.5. A solução deve ter suporte a TLS 1.3.

ITEM	DESCRIÇÃO	UNIDADE DE MEDIDA	QUANT.
3	CAPACIDADE ADICIONAL PARA SOLUÇÃO EM FIREWALL DE APLICAÇÕES WEB	UN	28

3.3.1. Pacote de Capacidade Adicional, deverá entregar um upgrade de licença para expansão do Throughput da solução do ITEM 1 de, no mínimo, de 3 GBPS.

3.3.2. SUPORTE E GARANTIA;

a) A(s) licença(s) deverá(ão) ser acompanhada(s) de Garantia do Fabricante para o período de 60 meses com suporte, na modalidade 24x7;

b) Os serviços de suporte serão fornecidos conforme ITEM 9.1 deste Termo de Referência

3.3.3. Caso a solução ofertada não utilize esta modalidade de licenciamento ou em que as funcionalidades deste item já estejam contempladas em um dos demais contidos no lote, demonstrados na proposta, o valor do item deverá figurar como R\$ 0,01 (um centavo) e ele não poderá ser adquirido por adesão.

ITEM	ESPECIFICAÇÃO	UNIDADE DE MEDIDA	QUANT.
4	SERVIÇO DE INSTALAÇÃO E REPASSE DE CONHECIMENTO HANDS-ON	UN	20

Especificação técnica mínima

3.4.1. Serviço de instalação: os serviços de instalação física, lógica serão executados pela CONTRATADA e deverão ser estruturados conforme as fases a seguir.

3.4.1.1. Fase de abertura:

- Validar e Homologar escopo do projeto;
- Validar objetivos e premissas do projeto;
- Validar riscos e restrições do projeto;
- Identificar e validar os requisitos do projeto;
- Efetuar o levantamento de informações sobre o ambiente atual, em complementação ao conjunto de informações apresentado nesta especificação técnica;
- Efetuar o gerenciamento de mudanças, contemplando análise de riscos de implementação do sistema;
- Apresentar o estudo dos riscos envolvidos na migração para o novo sistema a ser implantado.

3.4.1.2. Fase de planejamento:

- Elaborar plano de projeto;
- Definir as pessoas envolvidas por parte da CONTRATANTE no projeto;
- Reunir as equipes da CONTRATADA e CONTRATANTE;
- Definir os parâmetros de configuração básicos e avançados a serem implementados;

- e) Apresentar o Mapa de rede contendo a topologia a ser implementada;
- f) Apresentação do cronograma do projeto com os prazos e responsabilidades;
- g) Verificar os pré-requisitos do projeto;
- h) Apresentar plano do projeto para a homologação por parte da CONTRATANTE.

3.4.1.3. Fase de execução: O serviço de instalação consiste na colocação do(s) equipamento(s) em pleno funcionamento, em conformidade com o disposto nesta especificação técnica, no Edital e seus Anexos e em perfeitas condições de operação, de forma integrada ao ambiente de infraestrutura de informática da CONTRATANTE e deve contemplar, no mínimo, o seguinte:

- a) Deverão ser realizados por conta da contratada o armazenamento, a embalagem, o transporte, a entrega e a instalação de todo e qualquer item do objeto do edital, de tal maneira que a contratada será responsável pela remessa de todos os equipamentos para o(s) endereços informados no Edital, nos quais a solução de segurança será efetivamente implantada.
- b) A CONTRATADA deverá efetuar instalação e configuração realizada de acordo com as recomendações do fabricante (recommended settings);
- c) A CONTRATADA deverá efetuar a instalação do appliance virtual ou físico (conforme item solicitado) na infraestrutura indicada pelo CONTRATANTE, onde a configuração realizada deverá estar em conformidade com as recomendações do fabricante (recommended settings);
- d) Conexão e configuração de todos os equipamentos e/ou componentes da solução da rede do CONTRATANTE, inclusive configuração de VLANs e interfaces virtuais, se for o caso;
- e) Atualização de softwares, firmwares e drivers que compõem a solução;
- f) A CONTRATADA deverá fornecer, quando for o caso, todos os equipamentos, componentes, acessórios e cabos de conexão para interligar fisicamente todos os componentes da solução entregue;
- g) Aplicação das licenças necessárias à solução entregue;
- h) Testes da solução, incluindo testes de failover;
- i) Documentação do ambiente configurado e instalado.

3.4.2. Os serviços de instalação e configuração deverão se basear nas melhores práticas estabelecidas pelo respectivo fabricante em seus manuais de instalação e configuração ou artigos técnicos.

3.4.3 A solução, deverá ser entregue com todas as funcionalidades, recursos, componentes, acessórios, softwares e licenciamentos necessários ao seu pleno funcionamento.

3.4.4. Todas as informações necessárias à implantação, como topologia de rede, VLANs, endereçamento IP, portas de Swtichs que devem ser utilizadas e outras necessárias à perfeita configuração, interligação e funcionamento da solução serão fornecidas pelo CONTRATANTE.

3.4.5. A instalação da solução, incluindo todos os componentes e acessórios, será realizada pela CONTRATADA, com acompanhamento de uma equipe destacada pela CONTRATANTE.

3.4.6. A CONTRATADA deverá providenciar um profissional certificado pelo fabricante na solução para garantir a conformidade da instalação e a configuração dos equipamentos e softwares que compõem a solução.

3.4.7. A instalação, configuração e testes do equipamento deverá ser feita com o acompanhamento de técnicos da CONTRATANTE, visando o repasse de conhecimento e observados os padrões de gerenciamento de manutenção e segurança da CONTRATANTE.

3.4.8. A CONTRATADA deverá efetuar a instalação/configuração conforme a definição da arquitetura de cada sistema, envolvendo pelo menos:

- a) O agrupamento dos "appliances" em configuração do tipo "cluster" do tipo ativo/ativo ou ativo/passivo;
- b) Segmentação das redes por meio do uso de VLANs;
- c) Definição das redes IP a serem empregadas pelos servidores reais (redes de serviço);
- d) A criação de usuários para fins de operação e administração do sistema.
- e) Configuração de alarmes e notificações automatizadas a serem enviadas via protocolos SNMP e/ou SMTP.
- f) Configuração da topologia de conectividade de rede entre o sistema e os ativos de rede em operação nos datacenters do contratante
- g) Instalação, registro e ativação de licenças para todos os equipamentos ofertados, em total conformidade com essa especificação técnica.
- h) Teste e homologação do conjunto de recursos e funcionalidades do sistema implantado.

3.4.9. A critério do CONTRATANTE, os serviços poderão ser executados fora do horário comercial e/ou em finais de semana ou feriados sem custo adicional para o contratante, visando minimizar os transtornos aos usuários devido a uma eventual indisponibilidade dos serviços. Por conseguinte, as atividades que não tenham impacto de indisponibilidade ou que não venham a requerer a parada dos equipamentos poderão ser executadas em horário comercial. Para as atividades que tenham impacto de disponibilidade ou que venham a requerer a parada dos equipamentos deverão ser executadas fora do horário de expediente, inclusive em feriados ou finais de semana, de acordo com o estabelecido entre a CONTRATADA e o CONTRATANTE.

3.4.9.1. Atividades associadas à implantação com a necessidade de interrupção de serviços em produção, deverão ocorrer fora do expediente normal do Tribunal e estarão sujeitas ao planejamento e aprovação prévia da equipe técnica da CONTRATANTE.

3.4.10. O serviço de implantação da solução deverá ser concluído no prazo de, no máximo, 30 (trinta) dias, contados a partir da confirmação do recebimento da Ordem de Serviço.

3.4.10.1. Para todos os efeitos, a conclusão dos serviços de instalação e configuração será atestada pela entrega do sistema em pleno funcionamento, incluindo documentação "As Built", contendo planejamento, relatório de

instalação, configuração adotada, testes realizados e seus resultados, de acordo com as especificações do(s) fabricante(s) e demais condições estabelecidas nesta especificação técnica.

3.4.11. Características do repasse de conhecimento hands-on: as atividades de instalação deverão ser acompanhadas na modalidade hands-on, devendo a CONTRATADA:

a) Efetuar o repasse hands-on com carga horária de, no mínimo, 6 (seis) horas para o repasse de conhecimento referente à integração da solução e sua implantação com a transferência das informações básicas de configuração e operação;

b) O repasse de informações deverá cobrir conhecimentos mínimos necessários para administração, configuração, otimização, resolução de problemas e utilização da solução;

c) A equipe técnica do Tribunal, responsável pela infraestrutura técnica deverá disponibilizar no mínimo 2(dois) e no máximo 6(seis) técnicos para o acompanhamento das atividades de hands-on.

3.4.11.1. As horas do acompanhamento hands-on deverão ser distribuídas ou organizadas da melhor maneira durante as atividades de instalação/configuração, mediante proposição da equipe técnica do Tribunal, com a anuência da fiscalização do Contrato.

3.4.11.2. Condições de aceitação do repasse hands-on

3.4.11.2.1. Não serão recebidos os serviços de hands-on prestados por profissionais que não estejam hábeis a demonstrar na prática as funcionalidades principais da solução WAF, particularmente, as atividades relacionadas à mudança de configuração e operação da solução.

3.4.11.2.2. A não aceitação do hands-on implicará a não aceitação da entrega definitiva do serviço (ITEM 4).

3.4.11.3. Todas as despesas de instrutor(es), deslocamento de instrutor(es) e demais itens relacionados ao repasse Hands-On, serão de responsabilidade da CONTRATADA.

ITEM	ESPECIFICAÇÃO	UNIDADE DE MEDIDA	QUANT
5	TREINAMENTO ESPECIALIZADO	UN	90

Especificação técnica mínima

3.5.1. Trata-se do serviço de treinamento da solução, na modalidade de fornecimento de voucher para treinamento, cujo escopo do treinamento cubra conceitos de configuração, operação, administração, gerência, otimização, resolução de problemas e gestão de todos os componentes da solução de forma que o(s) servidor(es) capacitado(s) possam colocar os equipamentos e softwares em produção, bem como planejar mudanças de configuração no ambiente.

3.5.1.a) O treinamento deverá oferecer carga horária total de no mínimo 20(vinte) horas.

3.5.1.b) Serão aceitos preferencialmente treinamentos nas modalidades online ao vivo (EAD), podendo os treinamentos online ao vivo serem gravados, a critério da CONTRATANTE.

3.5.1.c) A CONTRATADA deve prover capacitação técnica em turma com no mínimo 5 (cinco) e no máximo 8 (oito) participantes.

3.5.1.d) Se o treinamento for ofertado na modalidade EAD, deverá respeitar o limite de 4 (quatro) horas por dia.

3.5.1.e) O treinamento deverá cobrir conhecimentos necessários para instalação, administração, configuração, gerência, otimização, resolução de problemas e utilização da solução.

3.5.2. As despesas decorrentes do serviço de treinamento (instrutores, confecção do material didático, licenciamento de plataforma de videoconferência etc.) serão de exclusiva responsabilidade da CONTRATADA.

3.5.3. O treinamento poderá ser composto de mais de 1(um) módulo, que deverão ser discriminados na proposta da licitante.

3.5.4. A licitante deverá anexar a grade de treinamentos do fabricante, com a ementa do(s) curso(s), para comprovar que o(s) treinamento(s) ofertados atendem os requisitos indicados no item 3.5.1.e.

3.5.5. O Tribunal poderá planejar e escolher quaisquer das datas, ou períodos, dos eventos de capacitação no prazo de validade da ata de registro de preços, a contar da entrega do calendário.

3.5.6. O treinamento deverá ser ministrado em data oportuna a ser informada à fiscalização após ou antes da instalação dos equipamentos, ficando a critério da administração e baseando-se no calendário a ser fornecido pela contratada.

3.5.7. É permitido à CONTRATADA terceirizar o treinamento a outra que preste serviços de treinamento da solução ofertada, ou ao próprio fabricante, desde que mantidas as demais condições deste documento e permanecendo ela a única responsável pelo atendimento do contratado para todos os fins.

- 3.5.8. O treinamento deverá ser ministrado por profissionais certificados pelo fabricante (com a certificação mais alta do fabricante), cuja comprovação deverá ser encaminhada na assinatura do Contrato.
- 3.5.9. A contratada deverá fornecer material didático individual, na modalidade digital, que abranja todo o conteúdo do(s) curso(s). Todo o material didático oferecido pela Contratada para realização do treinamento, atualizado e poderá estar em inglês ou português.
- 3.5.10. O treinamento deve ser ministrado em português do Brasil. Caso não exista material oficial do produto em língua portuguesa, será aceito material em inglês.
- 3.5.11. O treinamento deverá oferecer acesso a laboratório prático virtual, fornecido pela contratada, para configuração e execução de exercícios práticos.
- 3.5.11.1. No ambiente de treinamento, os servidores indicados pelo CONTRATANTE devem ter acesso em ambiente de laboratório a todos os produtos ofertados (ou similares) para realização da capacitação.
- 3.5.11.2. Após a conclusão da capacitação, o ambiente EAD deverá permanecer disponível ao acesso do aluno por um prazo mínimo de 12(doze) meses, sob demanda do CONTRANTE.
- 3.5.12. A Contratada deverá emitir para o servidor participante, sem ônus para o Tribunal e no prazo máximo de até 10 (dez) dias úteis após o término do treinamento, o certificado de conclusão, no qual deverá constar o nome do treinando, a data, o local e a carga horária. A cópia deste certificado deverá acompanhar a nota fiscal/fatura para o devido pagamento.
- 3.5.13. A ausência do servidor ao treinamento é de responsabilidade do Tribunal, cabendo à contratada informar no certificado a carga horária e assiduidade do servidor.
- 3.5.14. A Contratada deverá aplicar o Formulário de Satisfação, conforme modelo de formulário constante no Anexo III deste Termo de Referência.
- 3.5.14.a) No Formulário, será utilizada escala de até 4 (quatro) pontos para cada quesito do formulário. No mínimo 70% dos participantes deverão atribuir grau igual ou superior a 3 (três), para o item avaliado ser considerado proveitoso.
- 3.5.14.b) O resultado da Avaliação de Instrutor será utilizado como critério de aceitação do treinamento, devendo ser considerado pela amostra de participantes como “proveitoso” para no mínimo 04(quatro) dos 07(sete) itens avaliados;
- 3.5.14.c) Caso o resultado da Avaliação de Instrutor seja considerado “não proveitoso”, o treinamento fornecido será considerado não aceito;
- 3.5.14.d) Na hipótese de não aceitação, a CONTRATADA deve oferecer outro treinamento, com a mesma carga horária, com outro instrutor, sem qualquer ônus para o CONTRATANTE;
- 3.5.14.e) Na hipótese de o resultado do segundo treinamento ser “não proveitoso”, o objeto será considerado não aceito, aplicando-se as sanções previstas contratualmente.

ITEM	ESPECIFICAÇÃO	UNIDADE DE MEDIDA	QUANT.
6	SERVIÇO DE OPERAÇÃO ASSISTIDA	UN	19

Especificação técnica mínima

- 3.6.1. Entende-se por Operação Assistida o acompanhamento e monitoramento remoto (não presencial) pela CONTRATADA da solução em produção, durante 10 (dez) dias úteis contínuos, imediatamente após a fase de implantação da solução, visando atender, operar e solucionar todas as dúvidas e problemas que possam ocorrer.
- 3.6.2. A CONTRATADA deverá apoiar o início das atividades técnicas da nova solução, garantindo apoio imediato e acesso rápido às soluções para alterar ou aplicar configurações necessárias ao ajuste, caso necessário, do ambiente de produção.
- 3.6.3. A CONTRATADA deverá manter à disposição da CONTRATANTE, durante o período de operação assistida, pessoal técnico especializado e qualificado para o acompanhamento e verificação do desempenho operacional e eliminação imediata de eventuais falhas detectadas no sistema.
- 3.6.4. A equipe técnica da CONTRATADA, a qual será responsável pela prestação dos serviços de Operação Assistida, deverá possuir certificação pelo fabricante de cada sistema fornecido/implantado.
- 3.6.5. O serviço de Operação Assistida deverá monitorar o ambiente da CONTRATANTE em horário a ser definido pela CONTRATANTE, podendo ser no período matutino, vespertino ou noturno, não excedendo 8h (oito horas) por dia.
- 3.6.6. A contratada deverá propor e tomar todas as ações necessárias para a prevenção da repetição das falhas que ocorrerem durante o período de execução dos serviços de operação assistida.
- 3.6.7. A CONTRATADA deverá realizar os ajustes necessários para assegurar a disponibilidade e desempenho do ambiente, devendo, ao final dos serviços, emitir relatório com os seguintes dados: (i) Uso computacional e de capacidade do ambiente; (ii) Problemas ocorridos durante o período, as soluções adotadas; (iii)

Disponibilidade do ambiente.

4 APRESENTAÇÃO DA PROPOSTA

4.1. Somente serão classificadas as propostas cujos produtos/serviços atendam às especificações mínimas descritas neste Termo de Referência;

4.2. Nos preços propostos deverão estar inclusos todas as despesas para seu fornecimento, como: transportes, tributos, etc;

4.3. A proposta da licitante deverá vir acompanhada de documentação técnica que comprove o atendimento de todos os requisitos deste termo de referência. Para tal, deverá ser indicado na proposta comercial os part number(s) referente(s) (PartNumbers/SKUs) a cada software(s) fornecido(s), licenças de uso e garantia do produto. Adicionalmente, **a licitante deverá indicar, ponto a ponto, qual seção da documentação técnica comprova o atendimento de cada requisito e conformidade do material proposto** com a especificação exigida deste termo de referência, evitando a pura transcrição do disposto neste Termo de Referência para a proposta;

4.4. A LICITANTE deverá indicar em sua proposta os fabricantes, modelos e versões de todos os componentes das soluções, incluindo componentes de hardware (se houver) e de software, realizando a indicação de todos os Códigos de Produto. Devem ser entregues prospectos/folders/folhetos com as características técnicas dos equipamentos, softwares e licenças. Devem ser apresentadas, de forma clara e detalhada, as descrições das soluções com todos os seus componentes (hardware e software), podendo ser complementadas por documentações integrantes da proposta, tais como: brochuras, catálogos, manuais técnicos, manuais de operação, etc. Na especificação técnica devem ser destacados e referenciados pelo licitante os requisitos mínimos exigidos no Termo de Referência, com a indicação do documento e página onde se encontra grifada a comprovação, sob pena de desclassificação;

4.5. A LICITANTE garantirá que o bem, quer seja de sua fabricação ou integralmente ou parcialmente de subfornecedores, estará exatamente de acordo com estas especificações, isentos de defeitos de fabricação, de matéria prima ou mão de obra. Deverá, também, ser informado o prazo de garantia, conforme especificado neste Termo de Referência;

4.6. A proposta deverá possuir validade mínima de 60 (sessenta) dias.

4.7. Os quantitativos e os valores máximos de referência para a licitação são os seguintes:

GRUPO 1 - SOLUÇÃO DE WEB APPLICATION FIREWALL(WAF)						
ITEM	DESCRIÇÃO	CATMAT/ CATSER	UNIDADE DE MEDIDA	QUANTIDADE (A)	VALOR UNITÁRIO (B)	VALOR GLOBAL (C)
1	FORNECIMENTO DE SOLUÇÃO DE WEB APPLICATION FIREWALL(WAF), DO TIPO APPLIANCE VIRTUAL, COM GARANTIA DE 60(SESENTA) MESES.	27464	UN	28	R\$ 506.996,66	R\$ 14.195.906,48
2	FORNECIMENTO DE SOLUÇÃO DE WEB APPLICATION FIREWALL(WAF), DO TIPO APPLIANCE FÍSICO, COM GARANTIA DE 60(SESENTA) MESES.	27472	UN	20	R\$ 904.583,67	R\$ 18.091.673,40
3	CAPACIDADE ADICIONAL PARA SOLUÇÃO EM	27464	UN	28	R\$ 185.181,67	R\$ 5.185.086,76

	FIREWALL DE APLICAÇÕES WEB					
4	SERVIÇO DE INSTALAÇÃO E REPASSE DE CONHECIMENTO HANDS-ON	27324	UN	20	R\$ 52.282,38	R\$ 1.045.647,60
5	TREINAMENTO ESPECIALIZADO	27260	UN	90	R\$ 28.330,00	R\$ 2.549.700,00
6	SERVIÇO DE OPERAÇÃO ASSISTIDA	27324	UN	19	R\$ 32.666,67	R\$ 620.666,73
VALOR GLOBAL DO LOTE (D)						R\$ 41.688.680,97

Tabela 4 - Modelo de proposta - Bens e serviços que compõem a solução

5. ESTRATÉGIA DA CONTRATAÇÃO

5.1 Regime, Tipo e Modalidade da Licitação

- O certame se realizará na forma licitação tradicional, na modalidade PREGÃO ELETRÔNICO SISTEMA DE REGISTRO DE PREÇOS, do tipo MENOR PREÇO GLOBAL.

5.2 Da aplicação de direitos de preferência::

- Nos termos da legislação vigente, conforme previsão em Edital, nas aquisições de bens e serviços de informática e automação definidos pela Lei nº 8.248, de 1991, será assegurado o direito de preferência conforme procedimento estabelecido nos artigos 5º e 8º do Decreto nº 7.174, de 2010. Sendo que as licitantes qualificadas como microempresas ou empresas de pequeno porte que fizerem jus ao direito de preferência terão prioridade no exercício desse benefício em relação às médias e às grandes empresas na mesma situação.

5.3. Critérios de Julgamento das Propostas

5.3.1. Durante a apresentação da proposta, a licitante deverá demonstrar que o produto ofertado atende às exigências solicitadas nesta especificação. Para esta comprovação, serão aceitos catálogos, *datasheets*, manuais, sites ou outra documentação oficial onde se possa identificar de maneira inequívoca o modelo de equipamento proposto.

5.3.2. Em caso de dúvidas na comprovação da especificação, poderão ser solicitados por meio de diligência, esclarecimentos sobre a especificação dos produtos cotados pela licitante.

5.3.3. A licitante deverá apresentar declaração de que o produto atende a todas especificações exigidas.

5.4 . Critérios de Qualificação Técnica para a Habilitação

5.4.1. A LICITANTE deverá apresentar atestado(s) de capacidade técnica, fornecido(s) por pessoa jurídica de direito público ou privado, que comprove que já realizou **o fornecimento de, pelo menos, 01 (um) appliance virtual e/ou físico da solução Web Application Firewall (WAF), incluindo a execução ou prestação destes serviço(s) de implantação e configuração de solução Web Application Firewall (WAF)**, a fim de comprovar a qualificação técnica para desempenho de atividade pertinente e compatível com o objeto da licitação.

5.4.2. Os atestados deverão conter as seguintes informações mínimas: nome e cargo da pessoa que os assina, quantitativo associado ao fornecimento, valor e/ou Contrato(s) associado(s) à da prestação dos serviços;

5.4.3. A critério do pregoeiro, as licitantes deverão disponibilizar informações adicionais necessárias à comprovação da legitimidade do(s) atestado(s) apresentado(s), inclusive cópia de pelo menos uma nota fiscal do serviço constante no documento apresentado.

5.4.4. Conforme art. 43, §3º da Lei nº 8.666/93, os conteúdos dos atestados/declarações serão objeto de averiguação pelo TRE-PA, mediante diligências.

5.4.5. Ainda, em termos de diligência, o TRE-PA se reserva ao direito de entrar em contato com os gestores do contrato, realizar visita(s) ou reuniões com as entidades emissoras de forma a sanar dúvidas e atestar a veracidade das informações apresentadas. Devido a tal, todas as informações necessárias à comprovação da legitimidade dos atestados solicitados

poderão ser solicitadas para averiguação. Quais sejam: cópia do contrato que deu suporte à contratação, Relatórios Técnicos de Controle ou Execução do Contrato, Notas Fiscais, Ordens de Serviço, endereço e telefones dos gestores do contrato e local em que foram prestados os serviços.

5.5. Documentação exigida - Fase contratual

5.5.1. A CONTRATADA deverá apresentar após assinatura do contrato, no prazo de até 10 (dez) dias contados da publicação do extrato do Contrato no Diário Oficial da União, a documentação associadas ao(s) profissional(is) envolvidos e certificações mínimas associadas à execução dos serviços, conforme os itens a seguir.

5.5.2. A licitante contratada deverá apresentar analista (s) integrador (es) – conjunto com um ou mais profissionais, certificados pelo fabricante da solução, que individualmente ou conjuntamente serão responsáveis pelos serviços de implantação e transferência tecnológica.

5.5.3. As certificações profissionais serão auditadas no início dos serviços pela fiscalização do Contrato.

5.5.4. Nos casos da CONTRATADA não apresentar as certificações ou das certificações apresentadas não corresponderem às solicitadas, o CONTRATANTE terá autonomia para solicitar a troca do profissional indicado a qualquer tempo. O TRE-PA não autorizará o início dos serviços enquanto não for apresentado técnico certificado.

5.5.5. Após o recebimento do pedido de instalação, a contratada terá 5 (cinco) dias úteis para informar o técnico que fará a instalação acompanhada da comprovação da certificação exigida.

5.6. Dotação Orçamentária

5.6.1. As despesas para contratação do objeto deste Termo de Referência correrão por conta das seguintes referências de orçamento, correspondente aos exercícios associados à vigência da ata de registro de preços:

- Elemento de Despesa 44.90.40 - EQUIPAMENTOS DE TIC - SEGURANÇA DA INFORMAÇÃO (SIN EQUITIC);
- Elemento de Despesa 33.90.40 - APOIO TECNICO E OPERACIONAL DE TIC (TIC APOIO).

5.7 Critérios Sociais e Culturais

5.7.1. Todos os manuais, guias de instruções e ajuda deverão ser disponibilizados preferencialmente para o idioma Português do Brasil - PtBR e fornecidos em meio digital.

5.7.2. O licenciamento e o suporte devem ser prestados preferencialmente no idioma português do Brasil.

5.7.3. Os softwares aplicativos e interface do software devem ter a possibilidade de escolha de idioma pelo usuário. Será admitido o idioma inglês somente quando não existir uma versão no idioma português do Brasil.

5.7.4. Os profissionais da CONTRATADA deverão trajar-se de maneira respeitável e usar linguagem respeitosa e formal no trato com os servidores do órgão, Gestão Contratual e os dirigentes da CONTRATANTE.

5.8 Critérios de Segurança da Informação

5.8.1. Manutenção de Sigilo e Normas de Segurança

- A Contratada deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.
- O Termo de Compromisso, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal da Contratada, e Termo de Ciência, a ser assinado por todos os empregados da Contratada diretamente envolvidos na contratação, encontram-se nos ANEXOS I - TERMO DE COMPROMISSO E MANUTENÇÃO DE SIGILO e ANEXO II - TERMO DE CIÊNCIA.

5.9. Quantitativos a serem registrados

TRIBUNAL	ITEM 1 - Fornecimento	ITEM 2 - Fornecimento	ITEM 3 - Capacidade	ITEM 4 - Serviço de	ITEM 5 - Treinamento	ITEM 6 -
----------	-----------------------	-----------------------	---------------------	---------------------	----------------------	----------

	de Solução de Web Application Firewall(WAF), do tipo Appliance Virtual, com suporte e garantia de 60(sessenta) meses.	de Solução de Web Application Firewall(WAF), do tipo Appliance Físico, com suporte e garantia de 60(sessenta) meses.	adicional para solução em firewall de aplicações web.	instalação e repasse de conhecimento hands-on	especializado	Serviço de operação assistida
TRE-PA	2	2	2	1	6	1
TRE-RJ	0	2	0	1	5	1
TRE-SP	2	2	2	2	6	2
TRE-SE	2	0	2	1	1	1
TRE-PR	2	2	2	1	6	1
TRE-TO	2	0	2	1	6	1
TRE-DF	2	0	2	1	5	1
TRE-PB	2	0	2	1	6	1
TRE-PE	0	2	0	1	2	1
TRE-AM	0	2	0	1	4	1
TRE-SC	2	0	0	1	6	1
TRE-AC	2	0	2	1	4	1
TRE-MS	0	2	0	1	1	1
TRE-RN	0	2	2	1	5	0
TRE-CE	2	2	2	1	6	1
TRE-ES	2	0	2	1	8	1
TRE-RO	2	0	2	1	1	1
TRE-AP	2	2	2	1	6	1
TRE-GO	2	0	2	1	6	1
TOTAIS	28	20	28	20	90	19

5.10 Possibilidade de Adesão à Ata de Registro de Preços por outros órgãos

5.10.1. Será permitida a adesão aos Tribunais Regionais Eleitorais que não figuram como partícipes desta Ata de Registro de Preços, em razão da arquitetura proposta na Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).

5.11. Endereço do local de entrega e/ou de prestação do serviço de cada TRE, indicados como órgãos participantes

TRIBUNAL	ENDEREÇO DO LOCAL DE ENTREGA E/OU DE PRESTAÇÃO DO SERVIÇO
TRE-PA	Rua João Diogo, 288 - Bairro Campina- CEP 66015902 - Belém - PA
TRE-RJ	Av. Presidente Wilson, 194/198, 7o andar – Centro — Rio de Janeiro — RJ CEP 20.030-021
TRE-SP	Sede I: Seção de Rede e Servidores do TRE-SP, localizada na Rua Francisca Miquelina,123, Bairro Bela Vista, São Paulo - SP, CEP 01316-900 Sede II: Rua Doutor Falcão Filho, 121, Vale do Anhangabaú, São Paulo - SP, CEP01007-010.
TRE-SE	CENAF, Lote 7, Variante 2 - Bairro Capucho - Aracaju - SE - CEP 49081-000
TRE-PR	Rua João Parolin, 224, Bairro: Prado Velho, Cidade: Curitiba-PR, CEP: 80220-902
TRE-TO	Quadra 202 Norte, Av. Teotônio Segurado, Conjunto 01 Lotes 1 e 2 Plano Diretor Norte, Palmas-TO, CEP 77.006-214 .
TRE-DF	Praça Municipal de Brasília, Quadra 02, Lote 06, Zona Cívico-Administrativa, Brasília - DF, 70094-901
TRE-PB	Av. Princesa Isabel, 201- Tambiá - CEP 58020-528 - João Pessoa/PB
TRE-PE	Av. Gov. Agamenon Magalhães, no 1.160, Derby, Recife-PE - CEP 52.010-904 e prédio anexo do Entroncamento;
TRE-AM	Avenida André Araújo, no 200, Aleixo, Manaus-AM – CEP: 69060-000. Sede do Tribunal Regional Eleitoral do Amazonas/ Secretaria de Tecnologia da Informação.
TRE-SC	Rua Esteves Júnior, no 68 – Centro Florianópolis – Santa Catarina – CEP: 88015-130
TRE-AC	Alameda Ministro Miguel Ferrante, 224 - Bairro Portal da Amazônia - Rio Branco - AC/ CEP 69915-632
TRE-MS	Rua Delegado José Alfredo Hardman, 184, Parque dos Poderes, na cidade de Campo Grande/MS - CEP: 79037-106
TRE-RN	Avenida Rui Barbosa, 215 - Tirol - Natal/RN - CEP: 59.015-290
TRE-CE	R. Dr. Pontes Neto, s/n, Bairro: Luciano Calvancante, Fortaleza, CE - CEP: 60813-600
TRE-ES	Avenida João Baptista Parra, 575 Praia do Suá. Vitória - ES CEP: 29052-123
TRE-RO	Av. Presidente Dutra, 1889 - Bairro: Baixa da União, CEP 76.805-901 - Porto Velho/RO

TRE-AP	Avenida Mendonça Junior, 1502 - Centro, Macapá - AP - 68900-914 - Brasil.
TRE-GO	Tribunal Regional Eleitoral de Goiás - Secretaria de Tecnologia da Informação - Praça Cívica, nº 300 - Setor Central - Goiânia - GO - CEP 74.003-010 - 5o andar.

6. DEFINIÇÃO DAS OBRIGAÇÕES CONTRATUAIS

6.1. Definição das obrigações da contratante

6.1.1. A CONTRATANTE obriga-se a promover, por intermédio de Comissão ou servidor designado na forma do art. 67 da Lei n.º 8.666/93, o acompanhamento e a fiscalização da execução do objeto do contrato, conforme a seguir:

6.1.2. Receber o objeto no prazo e condições estabelecidas no Edital e seus anexos;

6.1.3. Anotar em registro próprio os defeitos detectados e comunicando as ocorrências de quaisquer fatos que, a seu critério, exijam o reparo ou substituição dos bens por parte da CONTRATADA.

6.1.4. Verificar minuciosamente, no prazo fixado, a conformidade dos bens recebidos provisoriamente com as especificações constantes do Edital e da proposta, para fins de aceitação e recebimento definitivo;

6.1.5. A existência de fiscalização da CONTRATANTE de modo algum atenua ou exime a responsabilidade da CONTRATADA por qualquer vício ou defeito presente nos bens fornecidos.

6.1.6. Abrir e acompanhar os chamados técnicos à contratada, elaborando relatórios mensais, constando as conformidades e desconformidades dos serviços prestados;

6.1.7. Comunicar à CONTRATADA, por escrito, sobre imperfeições, falhas ou irregularidades verificadas no objeto fornecido, para que seja substituído, reparado ou corrigido;

6.1.8. Acompanhar e fiscalizar o cumprimento das obrigações da CONTRATADA, através de comissão/servidor especialmente designado;

6.1.9. Efetuar o pagamento à CONTRATADA no valor correspondente ao fornecimento do objeto, no prazo e forma estabelecidos no Edital e seus anexos;

6.1.10. A Administração não responderá por quaisquer compromissos assumidos pela CONTRATADA com terceiros, ainda que vinculados à execução do presente Termo de Contrato, bem como por qualquer dano causado a terceiros em decorrência de ato da CONTRATADA, de seus empregados, prepostos ou subordinados.

6.2. Definição das obrigações da contratada

6.2.1. A CONTRATADA obriga-se a fornecer o material obedecendo rigorosamente às especificações discriminadas neste Termo de Referência.

6.2.2. A CONTRATADA obriga-se, ainda, a:

a) Manter, durante o fornecimento, todas as condições de habilitação e qualificação exigidas neste Termo de Referência;

b) Não transferir a outrem, no todo ou em parte, o objeto do contrato a ser firmado

6.2.3. A CONTRATADA deve cumprir todas as obrigações constantes no Edital, seus anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto e, ainda:

a) Efetuar a entrega do objeto em perfeitas condições, conforme especificações, prazo e local constantes no Edital e seus anexos, acompanhado da respectiva nota fiscal, na qual constarão as indicações referentes a: marca, fabricante, modelo e prazo de garantia;

b) Atender aos chamados técnicos no prazo estipulado pela contratante;

c) Responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com os artigos 12, 13 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990);

d) Substituir, reparar ou corrigir, às suas expensas, no prazo fixado neste Termo de Referência (item 9.2.3), o objeto com avarias ou defeitos;

e) Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

f) Responsabilizar-se integralmente pelo fiel cumprimento do objeto contratado, prestando todos os esclarecimentos que forem solicitados pela CONTRATANTE, cujas reclamações se obriga a atender.

7. EXECUÇÃO DO CONTRATO

7.1 Prazo de entrega

7.1.1. A entrega de equipamentos, licenças e conclusão de serviços devem obedecer os seguintes prazos:

7.1.1.1. ITEM 1: prazo de entrega de, no máximo, 30 (trinta) dias, contados a partir da confirmação do recebimento da Ordem de Fornecimento.

7.1.1.2. ITEM 2: prazo de entrega de, no máximo, 60 (sessenta) dias, contados a partir da confirmação do recebimento da Ordem de Fornecimento.

7.1.1.3. ITEM 3: prazo de entrega de, no máximo, 30 (trinta) dias, contados a partir da confirmação do recebimento da Ordem de Fornecimento.

7.1.1.4. ITEM 4: prazo de execução de, no máximo, 30 (trinta) dias, contados a partir da confirmação do recebimento da Ordem de Serviço.

7.1.1.5. ITEM 5: prazo de execução de, no máximo, 30 (trinta) dias, contados a partir da confirmação do recebimento da Ordem de Serviço.

7.1.1.6. ITEM 6: prazo de execução de, no máximo, 10 (dez) dias úteis contínuos, imediatamente após a fase de implantação da solução.

7.1.2. Os prazos de entrega, substituição e reposição admitem prorrogação, mantidas as demais cláusulas da contratação e da nota de empenho que não sofrerem influência dessa prorrogação, sendo assegurada a manutenção do equilíbrio econômico-financeiro da contratação, desde que ocorra um dos motivos previstos nos incisos I a VI do § 1º do Art. 57 da Lei n. 8.666/93, devendo ser requerida por escrito, justificadamente, e apresentada até o último dia do referido prazo.

7.2 Local de execução/entrega

7.2.1. Tribunal Regional Eleitoral do Pará (Sede), rua João Diogo 288, Campina, Belém- PA- CEP 66015-902, Anexo I, Seção de Serviços de Redes (SSR).

7.2.2. Para os órgãos participantes, a entrega e/ou prestação do serviço ocorrerá nos locais indicados na tabela constante do item 5.11 deste Termo de Referência.

7.3 Condições gerais do fornecimento

7.3.1. A entrega dos materiais deverá efetuar-se no local de entrega designado no item 7.2.1, de segunda a sexta-feira, no horário das 08 às 15h;

7.3.2. Todos os custos, ônus, e obrigações e encargos deverão ser arcados pela contratada para entrega dos equipamentos nos endereços descritos neste TR.

7.3.3. Havendo alteração no endereço de entrega, sem alteração do município, o mesmo será disponibilizado por ocasião da entrega da Nota de Empenho;

7.3.4. Os produtos definidos neste Termo deverão ser novos e sem utilização anterior, originais e de boa qualidade, livres de defeitos, imperfeições e outros vícios que impeçam ou reduzam a usabilidade, observando rigorosamente as características especificadas, devendo ser apresentados nas embalagens originais dos fabricantes, adequadas para proteger seu conteúdo contra danos durante o transporte até o local de entrega;

7.3.5. O fornecedor deverá apresentar a garantia correspondente a cada item, a contar da data de aceite efetuada pelo TRE-PA.

7.3.6. Comunicar o TRE-PA, com antecedência razoável, a entrega e execução de serviços associados ao item 7 do Termo de Referência, com o propósito de possibilitar agendamento e organização pela unidade responsável pela fiscalização destas atividades, evitando-se o comprometimento do regular funcionamento dos serviços do órgão.

8. FORMA DE PAGAMENTO

8.1. A CONTRATADA deverá apresentar ao Tribunal Regional Eleitoral do Pará Nota Fiscal/Fatura da própria empresa, na forma impressa ou eletrônica, a qual será encaminhada para pagamento após o recebimento e o aceite definitivo de material e serviços associados ao objeto. A Nota Fiscal poderá ser encaminhada por e-mail para o endereço eletrônico a ser informado oportunamente pela fiscalização.

8.1.1. Se optante pelo Simples Nacional, deverá ser apresentada a declaração de que trata o art. 6º da Instrução Normativa nº 1234/2012, em meio físico ou eletrônico assinado por certificação digital (não será aceito simples cópia digitalizada).

8.2. O pagamento será efetuado através de Ordem Bancária, mediante depósito na conta corrente da CONTRATADA, até o 10º (décimo) dia útil da data da liquidação da despesa, observado o estabelecido no art. 5º da Lei nº 8.666/93, e desde que não ocorra fator impeditivo provocado pela CONTRATADA.

8.3. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária de pagamento.

8.4. No caso do valor do pagamento não ultrapassar o limite de que trata o inciso II do art. 24, da Lei n.º 8.666/93, o mesmo deverá ser efetuado no prazo de até 5 (cinco) dias úteis, nas condições referidas acima.

8.5. Nenhum pagamento será efetuado à CONTRATADA enquanto pendente de liquidação qualquer obrigação financeira que lhe for imposta, em virtude de penalidade ou inadimplência, sem que isso gere direito ao pleito de reajustamento dos preços ou correção monetária.

9. GESTÃO DO CONTRATO

9.1. DA GARANTIA E DO SUPORTE TÉCNICO

9.1.1 A garantia refere-se ao período oficial de suporte da solução, fornecido por seu fabricante, compreendendo o fornecimento de atualizações e correções durante todo o ciclo de vida da versão fornecida do sistema operacional.

9.1.1.a. A vigência da garantia começará a contar a partir do recebimento definitivo pela Comissão indicada pelo Gestor do Contrato.

9.1.2.b. Durante a vigência da garantia, o fornecedor deverá comunicar ao CONTRATANTE eventual alteração do número telefônico ou do e-mail para abertura de chamados.

9.1.2. A Contratada deverá fornecer garantia técnica de pelo menos 60 (sessenta) meses para a solução, contados a partir da data de emissão do Termo de Recebimento Definitivo relativo à fase de instalação;

9.1.3. Os serviços de garantia técnica englobam todos os elementos de hardware e software da solução, incluindo a prestação de serviços de suporte técnico, assistência corretiva e atualização tecnológica, compreendendo a substituição de peças, componentes, acessórios e aplicativos que apresentem defeito, ou precisem ser atualizados durante este período, sem qualquer ônus adicional para o CONTRATANTE, obrigando-se a Contratada a manter os equipamentos e aplicativos permanentemente em perfeitas condições de funcionamento para a finalidade a que se destinam;

9.1.4. A garantia técnica compreenderá todas as funcionalidades da solução ofertada, tanto as descritas no Termo de Referência quanto as contempladas nos manuais e demais documentos técnicos, incluindo a atualização de versões de software;

9.1.5. Qualquer software ou equipamento com hardware defeituoso, peças quebradas, com defeito ou gastas pelo uso normal deverá ser substituído por outro de mesma marca e modelo e com as mesmas características técnicas ou superiores, novo e de primeiro uso, no prazo de 48 (quarenta e oito) horas a partir de notificação do CONTRATANTE;

9.1.6. A Contratada deverá apresentar no protocolo do CONTRATANTE, antes do início da vigência do serviço de garantia técnica, todos os dados necessários para o registro de chamados técnicos na Central de Atendimento da Contratada, tais como, e-mail, números de telefone e fax, etc;

9.1.7. Suporte Técnico durante o período de Garantia Técnica:

9.1.7.a. Durante o período de garantia técnica de 60 (sessenta) meses, a partir do recebimento definitivo da instalação, a Contratada deverá garantir o funcionamento de toda a solução, fornecer atualizações, prestar suporte técnico e atender aos chamados técnicos para manutenção;

9.1.7.b. A Contratada deverá comunicar formalmente ao Gestor do Contrato a disponibilidade de novas versões e releases das licenças de software e firmwares, reservando-se, à equipe técnica do CONTRATANTE, o direito de exigir a atualização sem que isso implique acréscimo aos preços contratados;

9.1.7.c. A manutenção corretiva será realizada em período integral, 7 (sete) dias por semana e 24 (vinte e quatro) horas por dia, após solicitação do CONTRATANTE;

9.1.8. A contratada deverá entregar no protocolo do CONTRATANTE, mensalmente, até o 5º (quinto) dia útil do mês subsequente, para fins de controle, Relatório Gerencial dos Serviços (RGS) realizado no mês anterior. Deverão constar, no mínimo, as seguintes informações:

9.1.8.a. Relação de todos os chamados técnicos ocorridos no mês anterior, incluindo data e hora do início e término do suporte; identificação do problema; criticidades; providências adotadas para o diagnóstico, solução provisória e solução definitiva; data e hora do início e término da solução definitiva; identificação do técnico do CONTRATANTE que solicitou e validou o chamado; identificação do técnico da Contratada responsável pela execução do chamado, bem como outras informações pertinentes;

9.1.8.b. Cada chamado técnico aberto será avaliado individualmente pelo Gestor do Contrato;

9.1.8.c. O serviço será considerado recebido pelo Gestor do Contrato quando do fechamento de cada chamado, desde que não reapareçam posteriormente ao fechamento inconformidades técnicas comprovadamente relacionadas ao chamado recebido;

9.1.8.d. O Gestor do Contrato emitirá a recusa em caso de verificação de impropriedades ou erros impeditivos de recebimento do serviço prestado. A Contratada deverá promover as correções necessárias, conforme diretrizes a serem estabelecidas pelo Gestor do Contrato, sem prejuízo de aplicação de penalidades previstas.

9.1.9. A Contratada deverá fornecer versão atualizada do manual e demais documentos técnicos sempre que houver atualização nos manuais, nos softwares ou nos equipamentos da solução.

9.1.10. A CONTRATANTE poderá realizar a aplicação de pacotes de correção e migração de versões e releases das licenças de software, quando lhe for conveniente, cabendo à Contratada orientar e colocar à disposição um técnico para contato em caso de dúvidas ou falhas. A CONTRATANTE reserva-se o direito de proceder a outras configurações, instalações ou conexões nos equipamentos, desde que tal iniciativa não implique danos físicos e lógicos aos equipamentos, sem que isto possa ser usado como pretexto pela Contratada para se desobrigar do suporte da solução.

9.1.11. A Contratada deverá garantir pleno funcionamento dos equipamentos e softwares, bem como atualizações,

responsabilizando-se por qualquer componente adicional que for identificado após a contratação, seja por motivos de interoperabilidade, compatibilidade ou quaisquer outros motivos que impeçam o funcionamento efetivo da solução contratada.

9.1.12. A Contratada deverá dispor de serviço de esclarecimento de dúvidas relativas à utilização dos equipamentos e de abertura de chamado técnico por e-mail ou por telefone 0800 (gratuito), ou telefone local por todo o período da garantia técnica.

9.1.13. A Contratada deverá garantir, sem quaisquer custos adicionais, as atualizações havidas nos equipamentos nas versões de software e firmware, inclusive releases, pelo prazo de vigência da garantia;

9.1.14. O serviço de garantia técnica deverá permitir o acesso do CONTRATANTE à base de dados de conhecimento do fabricante dos equipamentos, provendo informações, assistência e orientação para diagnósticos, avaliações e resolução de problemas, características dos produtos e demais atividades relacionadas à correta operação e funcionamento dos equipamentos.

9.1.15. As atualizações e correções (patches) do software e firmwares deverão estar disponibilizados via WEB.

9.1.16. Quando a garantia técnica for acionada, o atendimento deverá ser iniciado imediatamente, independente do meio utilizado. A cada abertura de chamado, a Contratada deverá fornecer ao CONTRATANTE um código identificador único para acompanhamento.

9.1.17. A Contratada deverá conceder acesso ao CONTRATANTE ao controle de atendimento para acompanhamento dos chamados técnicos, ficando o encerramento destes condicionados ao aceite do Gestor do Contrato.

9.2 Do Recebimento Provisório e Definitivo

9.2.1. A CONTRATANTE efetuará o recebimento do objeto contratado, provisoriamente, para efeito de posterior verificação da conformidade do objeto com a especificação, e definitivamente, após a verificação da qualidade e quantidade do objeto e consequente aceitação.

9.2.2. Em caso de rejeição total/parcial do objeto contratado, correção, substituição ou demais hipóteses de descumprimento de outras obrigações contratuais, avaliadas na etapa de recebimento, sujeitará a LICITANTE VENCEDORA à aplicação das sanções administrativas cabíveis.

9.2.3. Os bens poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser substituídos no prazo de 15 (quinze) dias corridos, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades.

9.3. Termo de recebimento provisório

9.3.1. O CONTRATANTE receberá provisoriamente o objeto contratado, mediante emissão de termo circunstanciado assinado pelas partes, em até 5 (cinco) dias após a entrega do objeto.

9.3.2. O recebimento provisório caberá ao agente fiscalizador especialmente designado para acompanhamento e fiscalização do contrato decorrente desta proposição.

9.3.3. A fiscalização do contrato procederá a observação da qualidade do objeto, registrando a data de entrega dos materiais e a data de emissão do termo de recebimento provisório, bem como anotará quaisquer ocorrências que impactem na avaliação da qualidade do fornecimento pela LICITANTE VENCEDORA.

9.4. Termo de recebimento definitivo

9.4.1. Os representantes da administração deverão conferir a qualidade e especificações funcionais dos equipamentos entregues e confrontá-las com as exigências editalícias, promoverem testes de desempenho (se for o caso), verificar licenças, registrar a data de entrega, emitir o recibo e o termo de recebimento definitivo, bem como registrar quaisquer ocorrências que impactem na avaliação da qualidade do fornecimento pela LICITANTE VENCEDORA.

9.4.2. O recebimento definitivo caberá ao agente fiscalizador especialmente designado para acompanhamento e fiscalização do contrato decorrente desta proposição.

9.4.3. O objeto contratado será rejeitado caso esteja em desacordo com as especificações constantes deste Termo de Referência, devendo a CONTRATANTE apontar por escrito esta ocorrência, onde detalhou as razões para deixar de emitir o termo de recebimento definitivo e indicará as falhas e pendências verificadas.

9.4.4. O recebimento definitivo do objeto não exclui nem reduz a responsabilidade da LICITANTE VENCEDORA com relação ao funcionamento e configuração divergente do especificado, durante todo o seu período de garantia.

9.4.5. Ficam designados para compor a comissão que efetuará o recebimento definitivo o agente fiscalizador e o gestor do contrato, bem como seus respectivos substitutos.

9.4 Sanções Administrativas

9.5.1. Ficará impedida de licitar e de contratar com a União e será descredenciada no SICAF, pelo prazo de até cinco anos, sem prejuízo das multas previstas em edital e no contrato e das demais cominações legais, garantido o direito à ampla defesa, a licitante que, convocada dentro do prazo de validade de sua proposta:

- a) Deixar de entregar a documentação exigida no Edital;
- b) Não assinar a Ata de Registro de Preços ou o contrato e/ou não receber a Ordem de Fornecimento e/ou de Serviço;
- c) Apresentar documento falso ou fizer declaração falsa;
- d) Causar atraso execução do objeto deste Pregão;
- e) Não manter a proposta, injustificadamente;
- f) Falhar ou fraudar na execução do contrato;
- g) Comportar-se de modo inidôneo;
- h) Cometer fraude fiscal.

9.5.2. Sem prejuízo das demais sanções previstas no art. 87 da Lei nº 8.666/93, pelo atraso injustificado e inexecução total ou parcial do objeto deste Pregão, a Administração do Tribunal Regional Eleitoral do Pará, poderá, garantida a defesa prévia, aplicar à licitante vencedora as seguintes sanções:

- a) Advertência, nas hipóteses de faltas leves, assim entendidas aquelas que não acarretem prejuízos para o TRE/PA;
- b) Multa compensatória de até 10% (dez por cento) sobre o valor global da Ata de Registro de Preços, na hipótese de recusa em assinar a Ata de Registro de Preços ou do contrato, na hipótese de recusa em assinar o instrumento de contrato;
- c) Multa compensatória de até 10% (dez por cento) sobre o valor global do respectivo material, na hipótese de recusa em receber a Ordem de Fornecimento e/ou de Serviço;
- d) Multa compensatória de até 10% (dez por cento) sobre o valor global do respectivo material, na hipótese de inexecução parcial ou total da obrigação.

9.5.3. Pelo atraso injustificado na execução do contrato, a CONTRATANTE deverá, garantida a defesa prévia, aplicar à licitante vencedora multa moratória de 0,2% (dois décimos por cento) por dia de atraso na entrega do material e/ou conclusão do serviço contratado, tomando por base o valor global do respectivo material, limitado a 10% (dez por cento).

9.5.3.1. O atraso injustificado na execução do contrato por período superior a 30 (trinta) dias, bem como deixar de manter todas as condições de habilitação, poderá ensejar a rescisão do contrato.

ANEXO I DO TERMO DE REFERÊNCIA TERMO DE COMPROMISSO E MANUTENÇÃO DE SIGILO

A Sociedade Empresária _____, CNPJ _____, por intermédio de seu representante legal abaixo assinado, _____, CPF _____, doravante designados simplesmente CONTRATADA e RESPONSÁVEL, se comprometem, por intermédio do presente TERMO DE COMPROMISSO, a não divulgar sem autorização, quaisquer Informações Confidenciais (conforme definido abaixo) em relação ao Projeto de “Contratação de solução de *Web Application Firewall* (WAF)”, e de propriedade do Tribunal Regional Eleitoral do Pará, CNPJ nº 05.703.755/0001-76, doravante designado TRE-PA, em conformidade com as seguintes cláusulas e condições:

1. Por este instrumento, a Contratada declara estar apta a aceitar e receber INFORMAÇÕES com respeito ao parque tecnológico do TRE-PA, comprometendo-se a manter absoluta confidencialidade destas INFORMAÇÕES, independente de solicitação expressa neste sentido pelo TRE-PA ou quaisquer de seus representantes;
2. As INFORMAÇÕES abrangidas por este termo são de natureza técnica, operacional, comercial, jurídica e financeira expressas de forma escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, ficando expressamente vedada sua divulgação a terceiros, a qualquer título;
3. As partes deverão restringir a divulgação das INFORMAÇÕES para o pessoal que estiverem diretamente envolvidos na sua utilização em razão do fornecimento das INFORMAÇÕES e da elaboração do serviço a ser fornecido, ficando vedado o intercâmbio destas INFORMAÇÕES com terceiros que não estejam diretamente envolvidos com a prestação dos serviços;
4. A CONTRATADA obriga-se a informar imediatamente o TRE-PA qualquer violação das regras de sigilo que tenha ocorrido por sua ação ou omissão, independentemente da existência de dolo, bem como de seus empregados, prepostos e prestadores de serviço;
5. A CONTRATADA deverá prestar obediência às políticas de segurança da informação vigentes no Tribunal Regional Eleitoral do Pará ou que poderão ser instituídas durante a vigência do contrato;

6. A não observância de quaisquer das disposições estabelecidas neste instrumento sujeitará a CONTRATADA aos procedimentos judiciais cabíveis relativos a perdas e danos que possam advir ao TRE-PA e aos seus usuários;
7. O descumprimento de quaisquer das cláusulas do presente Termo acarretará a responsabilidade civil e criminal de acordo com as leis aplicáveis dos que, comprovadamente, estiverem envolvidos no descumprimento ou violação.

Gestor do Contrato do TRE-PA: _____

Representante da Contratada: _____

Local, UF, de de

ANEXO II DO TERMO DE REFERÊNCIA
TERMO DE CIÊNCIA
IDENTIFICAÇÃO DO CONTRATO

CONTRATO N°:

OBJETO: “Aquisição de solução de *Web Application Firewall* (WAF) e balanceamento de carga, incluindo prestação de serviços de instalação e configuração, com garantia técnica de 60 (sessenta) meses”

Contratada:

CNPJ:

Representante da Contratada:

CPF:

Pelo presente instrumento, o(s) funcionário(s) abaixo qualificado(s) e assinado(s) declara(m):

- Ter plena ciência e conhecimento do Termo de Compromisso e Manutenção de Sigilo firmado pela CONTRATADA;
- Ter conhecimento de sua(s) responsabilidade(s) no que concerne ao sigilo que deverá ser mantido sobre as atividades desenvolvidas ou as ações realizadas no âmbito do Contrato Administrativo;
- Comprometer-se a guardar sigilo necessário sobre todas as informações que eventualmente venha(m) a tomar conhecimento;
- Comprometer-se a prestar obediência às políticas de segurança da informação vigentes no Tribunal Regional Eleitoral do Pará ou que poderão ser instituídas durante a vigência do contrato.

IDENTIFICAÇÃO E ASSINATURA DO(S) DECLARANTE(S)

Nome: CPF: _____

Função/Cargo: _____

Assinatura: _____

Nome: CPF: _____

Função/Cargo: _____

Assinatura: _____

Local, UF, de de .

ANEXO III DO TERMO DE REFERÊNCIA
AVALIAÇÃO DO ITEM 5 - TREINAMENTO ESPECIALIZADO
AVALIAÇÃO DE REAÇÃO

Curso:

Promotor:

Período:

Carga Horária:**Instrutor:****Objetivo:**

Para que possamos avaliar a qualidade do treinamento, assinale com um (X) na nota que melhor expressa sua opinião de acordo com a escala abaixo:

Grau de satisfação	Não atendeu	Atendeu parcialmente	Atendeu plenamente	Superou
Nota	1	2	3	4

I- PROMOTOR DO EVENTO		NOTA			
ITEM		1	2	3	4
1- Quanto à organização do evento					
2- Quanto à adequação das instalações					
3- Quanto à adequação dos recursos audiovisuais					
4- Quanto à qualidade do material didático					
II- CONTEÚDO PROGRAMÁTICO		NOTA			
ITEM		1	2	3	4
1- Quanto ao cumprimento do conteúdo programático					
2- Quanto ao detalhamento na abordagem dos tópicos					
3- Quanto à adequação da carga horária					
4- Quanto a adequação do conteúdo a sua necessidade de conhecimento					
III- INSTRUTOR		NOTA			
ITEM		1	2	3	4
1- Quanto ao domínio do assunto					

2- Quanto à relevância e atualidade dos conhecimentos difundidos				
3- Quanto à promoção de um ambiente favorável à aprendizagem				
4- Quanto à clareza e objetividade nas exposições				
5- Quanto à objetividade na administração do tempo				
6 – Quanto ao incentivo à participação da turma				
7 – Quanto à disponibilidade para o atendimento e o apoio aos alunos				
IV- APROVEITAMENTO	NOTA			
ITEM	1	2	3	4
1- Quanto à assimilação do conteúdo				
2-Quanto à adequação do conteúdo ao objetivo proposto por sua unidade de lotação				
V- COMENTÁRIOS E SUGESTÕES:				

Modelo de formulário - SGP/CODES/Seção de Treinamento e Desenvolvimento

ANEXO II DO EDITAL - ATA DE REGISTRO DE PREÇOS n.º __/20__

PERMITE ADESÃO: (X) SIM (para Tribunais Regionais Eleitorais que não figuram como partícipes desta Ata de Registro de Preços, em razão da arquitetura proposta na Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).

PROCESSO n.º:

GESTOR DA ATA:

UNIÃO FEDERAL, por intermédio do **TRIBUNAL REGIONAL ELEITORAL DO PARÁ**, inscrito no CNPJ(MF) sob o n.º 05.703.755/0001-76, situado na Rua João Diogo n.º 288, Cidade de Belém, Estado do Pará, representado por seu(sua) Diretor(a)-Geral, no uso da competência que lhe foi atribuída pelo inciso VII do art. 1º da Portaria n.º 19.597/2020 - TRE/PRE/DG/SGP/GABSGP, deste Tribunal, nos termos do art. 15 da Lei Federal 8.666/93 e Decreto n.º 7.892/2013, observadas, ainda, as demais normas legais aplicáveis.

UNIDADE GERENCIADORA: _____

TELEFONE: (91) 3346-_____	E-MAIL: _____@tre-pa.jus.br
----------------------------------	------------------------------------

DETENTOR DA ATA:

EMPRESA:	
CNPJ/MF:	
Inscrição Estadual:	Inscrição Municipal:
REPRESENTANTE:	
ENDEREÇO:	
TELEFONE:	E-MAIL:

PREGÃO n.º: ____/202__

OBJETO: Registro de preços de solução de web application firewall (waf) e balanceamento de carga, incluindo prestação de serviços de instalação e configuração, treinamento especializado e serviço de operação assistida, com garantia técnica de 60 (sessenta) meses

LOTE ÚNICO - ÓRGÃO GERENCIADOR E ÓRGÃOS PARTICIPANTES

ITEM	DESCRIÇÃO	PART NUMBER / MARCA/ MODELO/ FABRICANTE/ VERSÃO /	QUANTIDADE REGISTRADA	VALOR UNITÁRIO	VALOR TOTAL
1	FORNECIMENTO DE SOLUÇÃO DE WEB APPLICATION FIREWALL(WAF), DO TIPO APPLIANCE VIRTUAL, COM GARANTIA DE 60(SESENTA) MESES.			R\$	R\$
2	FORNECIMENTO DE SOLUÇÃO DE WEB APPLICATION FIREWALL(WAF), DO TIPO APPLIANCE FÍSICO, COM GARANTIA DE 60(SESENTA) MESES.			R\$	R\$
3	CAPACIDADE ADICIONAL PARA SOLUÇÃO EM FIREWALL DE APLICAÇÕES WEB			R\$	R\$
4	SERVIÇO DE INSTALAÇÃO E REPASSE DE CONHECIMENTO HANDS-ON			R\$	R\$
5	TREINAMENTO ESPECIALIZADO			R\$	R\$
6	SERVIÇO DE OPERAÇÃO ASSISTIDA			R\$	R\$

VALOR GLOBAL DO LOTE ÚNICO						RS
-----------------------------------	--	--	--	--	--	-----------

ÓRGÃO / INSTITUIÇÃO - UASG	QUANTIDADE REGISTRADA POR ITEM					
	ITEM 1 - Fornecimento de Solução de Web Application Firewall(WAF), do tipo Appliance Virtual, com suporte e garantia de 60(sessenta) meses.	ITEM 2 - Fornecimento de Ssolução de Web Application Firewall(WAF), do tipo Appliance Físico, com suporte e garantia de 60(sessenta) meses.	ITEM 3 - Capacidade adicional para solução em firewall de aplicações web.	ITEM 4 - Serviço de instalação e repasso de conhecimento hands-on	ITEM 5 - Treinamento especializado	ITEM 6 - Serviço de operação assistida
TRE-PA	2	2	2	1	6	1
TRE-RJ - UASG 70017	0	2	0	1	5	1
TRE-SP - UASG 70018	2	2	2	2	6	2
TRE-SE - UASG 70012	2	0	2	1	1	1
TRE- PR - UASG 70019	2	2	2	1	6	1
TRE- TO - UASG 70027	2	0	2	1	6	1
TRE- DF - UASG 70025	2	0	2	1	5	1
TRE- PB - UASG 70009	2	0	2	1	6	1
TRE- PE - UASG 70010	0	2	0	1	2	1
TRE- AM - UASG 70003	0	2	0	1	4	1
TRE- SC - UASG 70020	2	0	0	1	6	1

TRE-AC - UASG 70002	2	0	2	1	4	1
TRE-MS - UASG 70016	0	2	0	1	1	1
TRE-RN - UASG 70008	0	2	2	1	5	0
TRE-CE - UASG 70007	2	2	2	1	6	1
TRE-ES - UASG 70015	2	0	2	1	8	1
TRE-RO - UASG 70024	2	0	2	1	1	1
TRE-AP - UASG 70029	2	2	2	1	6	1
TRE-GO, UASG 70023	2	0	2	1	6	1

VALIDADE DA ATA: 12 (doze) meses, a contar da assinatura.

A sociedade empresária especificada acima, através de seu representante legal, obriga-se a informar ao contratante eventual mudança de endereço.

E por estar, assim, justo e avençado, depois de lido e achado conforme, foi o presente instrumento lavrado e assinado digitalmente pelas partes.

DO CADASTRO DE RESERVA

Constitui Anexo ao presente instrumento a Ata de Formação de Cadastro de Reserva constante do Sistema Compras governamentais, acessível publicamente em <http://comprasnet.gov.br/aceso.asp?url=/livre/Pregao/ata0.asp> (Inserir o Código UASG do TRE/PA, qual seja 070004, e o número da licitação), contendo o registro das licitantes que aceitaram cotar os bens ou serviços acima pelos preços ora registrados, nos termos do inciso II e § 1º do art. 11 do Decreto nº 7.892/2013 e alterações.

O Decreto nº 7.892/2013, em seu art. 11, inciso II, assim dispõe:

"Art. 11. Após a homologação da licitação, o registro de preços observará, entre outras, as seguintes condições:

(...)

II - será incluído, na respectiva ata na forma de anexo, o registro dos licitantes que aceitarem cotar os bens ou serviços com preços iguais aos da licitante vencedora na sequência da classificação do certame, excluído o percentual referente à margem de preferência, quando o objeto não atender aos requisitos previstos no [art. 3º da Lei nº 8.666, de 1993](#); [\(Redação dada pelo Decreto nº 8.250, de 2.014\)](#)"

(...)

§ 1º O registro a que se refere o inciso II do **caput** tem por objetivo a formação de cadastro de reserva no caso de impossibilidade de atendimento pelo primeiro colocado da ata, nas hipóteses previstas nos arts. 20 e 21. ([Redação dada pelo Decreto nº 8.250, de 2.014](#)).

(...)

Art. 20. O registro do fornecedor será cancelado quando:

I - descumprir as condições da ata de registro de preços;

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

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

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

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

Art. 21. 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; ou

II - a pedido do fornecedor.

ANEXO III DO EDITAL - CONTRATO N.º __/202_ (MINUTA)

CONTRATO N.º __ / __

TERMO DE CONTRATO DE FORNECIMENTO E PRESTAÇÃO DE SERVIÇOS, QUE ENTRE SI FAZEM A UNIÃO, POR INTERMÉDIO DO TRE/PA E _____.

CONTRATANTE: UNIÃO, por intermédio do **TRIBUNAL REGIONAL ELEITORAL DO PARÁ**, inscrito no CNPJ/MF sob o n.º 05.703.755/0001-76, situado na Rua João Diogo, n.º 288, Belém - Pará, representado por seu(sua) Diretor(a)-Geral [se for o caso, acrescentar o termo substituto], Sr(a). [nome do titular ou substituto], brasileiro(a), [estado civil], portador(a) do RG n.º _____ - SSP/_____, inscrito no CPF sob o n.º _____, no uso da competência que lhe foi delegada pela Portaria DG nº 19.597 de 08 de junho de 2020, deste Tribunal.

CONTRATADA: _____, inscrita no CNPJ/MF sob o n.º _____, estabelecida na _____, Tel.: (____) _____, E-mail: _____, neste ato representada por _____, brasileiro(a), [estado civil], portador(a) do RG n.º _____ - SSP/_____, inscrito no CPF sob o n.º _____, de acordo com a representação legal conferida por [contrato social/estatuto social/procuração] constante do evento _____ do processo administrativo SEI nº _____.

Os CONTRATANTES têm, entre si, justo e avençado, e celebram, por força do presente instrumento, o presente CONTRATO DE FORNECIMENTO E PRESTAÇÃO DE SERVIÇOS, mediante as seguintes cláusulas e condições:

CLÁUSULA PRIMEIRA – DO OBJETO

1.1. O presente contrato tem por objeto o fornecimento de solução de Web Application Firewall (WAF) e balanceamento de carga, incluindo prestação de serviços de instalação e configuração, treinamento especializado e serviço de operação assistida, com garantia técnica de 60 (sessenta) meses.

CLÁUSULA SEGUNDA - DA FUNDAMENTAÇÃO LEGAL E DA VINCULAÇÃO

2.1. Este contrato fundamenta-se nas Leis nº 10.520/2002 e nº 8.666/1993 bem como na Resolução TSE nº 23.234/2010, e alterações, e vincula-se ao Edital do Pregão Eletrônico nº __/20__, e seus Anexos, como se aqui estivessem integralmente transcritos, vinculando-se ainda aos termos da proposta da contratada constante do evento _____ do processo administrativo SEI nº _____.

CLÁUSULA TERCEIRA – DAS OBRIGAÇÕES DA CONTRATANTE

3.1. A CONTRATANTE obriga-se a:

3.1.1. Promover, por intermédio de Comissão ou servidor designado na forma do art. 67 da Lei nº 8.666/93, o acompanhamento e a fiscalização da execução do objeto do contrato.

3.1.2. Receber o objeto no prazo e condições estabelecidas no Edital e seus anexos.

3.1.3. Anotar em registro próprio os defeitos detectados e comunicando as ocorrências de quaisquer fatos que, a seu critério, exijam o reparo ou substituição dos bens por parte da CONTRATADA.

3.1.4. Verificar minuciosamente, no prazo fixado, a conformidade dos bens recebidos provisoriamente com as especificações constantes do Edital e da proposta, para fins de aceitação e recebimento definitivo.

3.1.5. A existência de fiscalização da CONTRATANTE de modo algum atenua ou exime a responsabilidade da CONTRATADA por qualquer vício ou defeito presente nos bens fornecidos.

3.1.6. Abrir e acompanhar os chamados técnicos à contratada, elaborando relatórios mensais, constando as conformidades e desconformidades dos serviços prestados.

3.1.7. Comunicar à CONTRATADA, por escrito, sobre imperfeições, falhas ou irregularidades verificadas no objeto fornecido, para que seja substituído, reparado ou corrigido.

3.1.8. Acompanhar e fiscalizar o cumprimento das obrigações da CONTRATADA, através de comissão/servidor especialmente designado.

3.1.9. Efetuar o pagamento à CONTRATADA no valor correspondente ao fornecimento do objeto, no prazo e forma estabelecidos no Edital e seus anexos.

3.1.10. A Administração não responderá por quaisquer compromissos assumidos pela CONTRATADA com terceiros, ainda que vinculados à execução do presente Termo de Contrato, bem como por qualquer dano causado a terceiros em decorrência de ato da CONTRATADA, de seus empregados, prepostos ou subordinados.

CLÁUSULA QUARTA – DAS OBRIGAÇÕES DA CONTRATADA

4.1. A CONTRATADA obriga-se a fornecer o material obedecendo rigorosamente às especificações discriminadas no Termo de Referência.

4.2. A CONTRATADA obriga-se, ainda, a:

a) Manter, durante o fornecimento, todas as condições de habilitação e qualificação exigidas no Termo de Referência.

b) Não transferir a outrem, no todo ou em parte, o objeto do contrato a ser firmado.

4.3. A CONTRATADA deve cumprir todas as obrigações constantes no Edital, seus anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto e, ainda:

a) Efetuar a entrega do objeto em perfeitas condições, conforme especificações, prazo e local constantes no Edital e seus anexos, acompanhado da respectiva nota fiscal, na qual constarão as indicações referentes a: marca, fabricante, modelo e prazo de garantia.

b) Atender aos chamados técnicos no prazo estipulado pela contratante.

c) Responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com os artigos 12, 13 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990).

d) Substituir, reparar ou corrigir, às suas expensas, no prazo fixado no Termo de Referência (item 9.2.3), o objeto com avarias ou defeitos.

e) Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

f) Responsabilizar-se integralmente pelo fiel cumprimento do objeto contratado, prestando todos os esclarecimentos que forem solicitados pela CONTRATANTE, cujas reclamações se obriga a atender.

CLÁUSULA QUINTA – DA EXECUÇÃO DO CONTRATO

5.1. PRAZO DE ENTREGA:

5.1.1. A entrega de equipamentos, licenças e conclusão de serviços devem obedecer os seguintes prazos:

5.1.1.1. ITEM 1: prazo de entrega de, no máximo, 30 (trinta) dias, contados a partir da confirmação do recebimento da Ordem de Fornecimento.

5.1.1.2. ITEM 2: prazo de entrega de, no máximo, 60 (sessenta) dias, contados a partir da confirmação do recebimento da Ordem de Fornecimento.

5.1.1.3. ITEM 3: prazo de entrega de, no máximo, 30 (trinta) dias, contados a partir da confirmação do recebimento da Ordem de Fornecimento.

5.1.1.4. ITEM 4: prazo de execução de, no máximo, 30 (trinta) dias, contados a partir da confirmação do recebimento da Ordem de Serviço.

5.1.1.5. ITEM 5: prazo de execução de, no máximo, 30 (trinta) dias, contados a partir da confirmação do recebimento da Ordem de Serviço.

5.1.1.6. ITEM 6: prazo de execução de, no máximo, 10 (dez) dias úteis contínuos, imediatamente após a fase de implantação da solução.

5.1.2. Os prazos de entrega, substituição e reposição admitem prorrogação, mantidas as demais cláusulas da contratação e da nota de empenho que não sofrerem influência dessa prorrogação, sendo assegurada a manutenção do equilíbrio econômico-financeiro da contratação, desde que ocorra um dos motivos previstos nos incisos I a VI do § 1º do Art. 57 da Lei n. 8.666/93, devendo ser requerida por escrito, justificadamente, e apresentada até o último dia do referido prazo.

5.2. LOCAL DE EXECUÇÃO/ENTREGA:

5.2.1. Tribunal Regional Eleitoral do Pará (Sede), Rua João Diogo 288, Campina, Belém- PA- CEP 66015-902, Anexo I, Seção de Serviços de Redes (SSR).

5.3. CONDIÇÕES GERAIS DO FORNECIMENTO:

5.3.1. A entrega dos materiais deverá efetuar-se no local de entrega designado no item 5.2.1, de segunda a sexta-feira, no horário das 08 às 15h.

5.3.2. Todos os custos, ônus, e obrigações e encargos deverão ser arcados pela contratada para entrega dos equipamentos nos endereços descritos no TR.

5.3.3. Havendo alteração no endereço de entrega, sem alteração do município, o mesmo será disponibilizado por ocasião da entrega da Ordem de Fornecimento/Serviço.

5.3.4. Os produtos deverão ser novos e sem utilização anterior, originais e de boa qualidade, livres de defeitos, imperfeições e outros vícios que impeçam ou reduzam a usabilidade, observando rigorosamente as características especificadas, devendo ser apresentados nas embalagens originais dos fabricantes, adequadas para proteger seu conteúdo contra danos durante o transporte até o local de entrega.

5.3.5. O fornecedor deverá apresentar a garantia correspondente a cada item, a contar da data de aceite efetuada pelo TRE-PA.

5.3.6. Comunicar o TRE-PA, com antecedência razoável, a entrega e execução de serviços associados ao item 7 do Termo de Referência, com o propósito de possibilitar agendamento e organização pela unidade responsável pela fiscalização destas atividades, evitando-se o comprometimento do regular funcionamento dos serviços do órgão.

5.4. ESPECIFICAÇÃO TÉCNICA:

5.4.1. As especificações técnica dos itens objeto do contrato estão presentes no item 3 do Termo de Referência.

5.5. DOCUMENTAÇÃO EXIGIDA - FASE CONTRATUAL:

5.5.1. A CONTRATADA deverá apresentar após assinatura do contrato, no prazo de até 10 (dez) dias contados da publicação do extrato do Contrato no Diário Oficial da União, a documentação associadas ao(s) profissional(is) envolvido(s) e certificações mínimas associadas à execução dos serviços, conforme os itens a seguir.

5.5.2. A CONTRATADA deverá apresentar analista(s) integrador(es) – conjunto com um ou mais profissionais, certificados pelo fabricante da solução, que individualmente ou conjuntamente serão responsáveis pelos serviços de implantação e transferência tecnológica.

5.5.3. As certificações profissionais serão auditadas no início dos serviços pela fiscalização do Contrato.

5.5.4. Nos casos da CONTRATADA não apresentar as certificações ou das certificações apresentadas não corresponderem às solicitadas, o CONTRATANTE terá autonomia para solicitar a troca do profissional indicado a qualquer tempo. O CONTRATANTE não autorizará o início dos serviços enquanto não for apresentado técnico certificado.

5.5.5. Após o recebimento do pedido de instalação, a CONTRATADA terá 5 (cinco) dias úteis para informar o técnico que fará a instalação acompanhada da comprovação da certificação exigida.

5.6. CRITÉRIOS SOCIAIS E CULTURAIS:

5.6.1. Todos os manuais, guias de instruções e ajuda deverão ser disponibilizados preferencialmente para o idioma Português do Brasil - PtBR e fornecidos em meio digital.

5.6.2. O licenciamento e o suporte devem ser prestados preferencialmente no idioma português do Brasil.

5.6.3. Os softwares aplicativos e interface do software devem ter a possibilidade de escolha de idioma pelo usuário. Será admitido o idioma inglês somente quando não existir uma versão no idioma português do Brasil.

5.6.4. Os profissionais da CONTRATADA deverão trajar-se de maneira respeitável e usar linguagem respeitosa e formal no trato com os servidores do órgão, Gestão Contratual e os dirigentes da CONTRATANTE.

5.7. CRITÉRIOS DE SEGURANÇA DA INFORMAÇÃO:

5.7.1. Manutenção de Sigilo e Normas de Segurança:

5.7.1.1. A CONTRATADA deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo CONTRATANTE a tais documentos.

5.7.1.2. O Termo de Compromisso, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal da CONTRATADA, e Termo de Ciência, a ser assinado por todos os empregados da CONTRATADA diretamente envolvidos na contratação, encontram-se nos ANEXOS I - TERMO DE COMPROMISSO E MANUTENÇÃO DE SIGILO e ANEXO II - TERMO DE CIÊNCIA, do Termo de Referência.

CLÁUSULA SEXTA – DA GESTÃO DO CONTRATO

6.1. DA GARANTIA E DO SUPORTE TÉCNICO:

6.1.1 A garantia refere-se ao período oficial de suporte da solução, fornecido por seu fabricante, compreendendo o fornecimento de atualizações e correções durante todo o ciclo de vida da versão fornecida do sistema operacional.

6.1.1.a. A vigência da garantia começará a contar a partir do recebimento definitivo pela Comissão indicada pelo Gestor do Contrato.

6.1.2.b. Durante a vigência da garantia, o fornecedor deverá comunicar ao CONTRATANTE eventual alteração do número telefônico ou do e-mail para abertura de chamados.

6.1.2. A CONTRATADA deverá fornecer garantia técnica de pelo menos 60 (sessenta) meses para a solução, contados a partir da data de emissão do Termo de Recebimento Definitivo relativo à fase de instalação.

6.1.3. Os serviços de garantia técnica englobam todos os elementos de hardware e software da solução, incluindo a prestação de serviços de suporte técnico, assistência corretiva e atualização tecnológica, compreendendo a substituição de peças, componentes, acessórios e aplicativos que apresentem defeito, ou precisem ser atualizados durante este período, sem qualquer ônus adicional para o CONTRATANTE, obrigando-se a CONTRATADA a manter os equipamentos e aplicativos permanentemente em perfeitas condições de funcionamento para a finalidade a que se destinam.

6.1.4. A garantia técnica compreenderá todas as funcionalidades da solução ofertada, tanto as descritas no Termo de Referência quanto as contempladas nos manuais e demais documentos técnicos, incluindo a atualização de versões de software.

6.1.5. Qualquer software ou equipamento com hardware defeituoso, peças quebradas, com defeito ou gastas pelo uso normal deverá ser substituído por outro de mesma marca e modelo e com as mesmas características técnicas ou superiores, novo e de primeiro uso, no prazo de 48 (quarenta e oito) horas a partir de notificação do CONTRATANTE.

6.1.6. A CONTRATADA deverá apresentar no protocolo do CONTRATANTE, antes do início da vigência do serviço de garantia técnica, todos os dados necessários para o registro de chamados técnicos na Central de Atendimento da CONTRATADA, tais como, e-mail, números de telefone e fax, etc.

6.1.7. Suporte Técnico durante o período de Garantia Técnica:

6.1.7.a. Durante o período de garantia técnica de 60 (sessenta) meses, a partir do recebimento definitivo da instalação, a CONTRATADA deverá garantir o funcionamento de toda a solução, fornecer atualizações, prestar suporte técnico e atender aos chamados técnicos para manutenção.

6.1.7.b. A CONTRATADA deverá comunicar formalmente ao Gestor do Contrato a disponibilidade de novas versões e releases das licenças de software e firmwares, reservando-se, à equipe técnica do CONTRATANTE, o direito de exigir a atualização sem que isso implique acréscimo aos preços contratados.

6.1.7.c. A manutenção corretiva será realizada em período integral, 7 (sete) dias por semana e 24 (vinte e quatro) horas por dia, após solicitação do CONTRATANTE.

6.1.8. A CONTRATADA deverá entregar no protocolo do CONTRATANTE, mensalmente, até o 5º (quinto) dia útil do mês subsequente, para fins de controle, Relatório Gerencial dos Serviços (RGS) realizado no mês anterior. Deverão constar, no mínimo, as seguintes informações:

6.1.8.a. Relação de todos os chamados técnicos ocorridos no mês anterior, incluindo data e hora do início e término do suporte; identificação do problema; criticidades; providências adotadas para o diagnóstico, solução provisória e solução definitiva; data e hora do início e término da solução definitiva; identificação do técnico do CONTRATANTE que solicitou e validou o chamado; identificação do técnico da Contratada responsável pela execução do chamado, bem como outras informações pertinentes.

6.1.8.b. Cada chamado técnico aberto será avaliado individualmente pelo Gestor do Contrato.

6.1.8.c. O serviço será considerado recebido pelo Gestor do Contrato quando do fechamento de cada chamado, desde que não reapareçam posteriormente ao fechamento inconformidades técnicas comprovadamente relacionadas ao chamado recebido.

6.1.8.d. O Gestor do Contrato emitirá a recusa em caso de verificação de impropriedades ou erros impeditivos de recebimento do serviço prestado. A CONTRATADA deverá promover as correções necessárias, conforme diretrizes a serem estabelecidas pelo Gestor do Contrato, sem prejuízo de aplicação de penalidades previstas.

6.1.9. A CONTRATADA deverá fornecer versão atualizada do manual e demais documentos técnicos sempre que houver atualização nos manuais, nos softwares ou nos equipamentos da solução.

6.1.10. A CONTRATANTE poderá realizar a aplicação de pacotes de correção e migração de versões e releases das licenças de software, quando lhe for conveniente, cabendo à CONTRATADA orientar e colocar à disposição um técnico para contato em caso de dúvidas ou falhas. A CONTRATANTE reserva-se o direito de proceder a outras configurações, instalações ou conexões nos equipamentos, desde que tal iniciativa não implique danos físicos e lógicos aos equipamentos, sem que isto possa ser usado como pretexto pela CONTRATADA para se desobrigar do suporte da solução.

6.1.11. A CONTRATADA deverá garantir pleno funcionamento dos equipamentos e softwares, bem como atualizações, responsabilizando-se por qualquer componente adicional que for identificado após a contratação, seja por motivos de interoperabilidade, compatibilidade ou quaisquer outros motivos que impeçam o funcionamento efetivo da solução contratada.

6.1.12. A CONTRATADA deverá dispor de serviço de esclarecimento de dúvidas relativas à utilização dos equipamentos e de abertura de chamado técnico por e-mail ou por telefone 0800 (gratuito), ou telefone local por todo o período da garantia técnica.

6.1.13. A CONTRATADA deverá garantir, sem quaisquer custos adicionais, as atualizações havidas nos equipamentos nas versões de software e firmware, inclusive releases, pelo prazo de vigência da garantia.

6.1.14. O serviço de garantia técnica deverá permitir o acesso do CONTRATANTE à base de dados de conhecimento do fabricante dos equipamentos, provendo informações, assistência e orientação para diagnósticos, avaliações e resolução de problemas, características dos produtos e demais atividades relacionadas à correta operação e funcionamento dos equipamentos.

6.1.15. As atualizações e correções (patches) do software e firmwares deverão estar disponibilizados via WEB.

6.1.16. Quando a garantia técnica for acionada, o atendimento deverá ser iniciado imediatamente, independente do meio utilizado. A cada abertura de chamado, a CONTRATADA deverá fornecer ao CONTRATANTE um código identificador único para acompanhamento.

6.1.17. A CONTRATADA deverá conceder acesso ao CONTRATANTE ao controle de atendimento para acompanhamento dos chamados técnicos, ficando o encerramento destes condicionados ao aceite do Gestor do Contrato.

6.2. DO RECEBIMENTO PROVISÓRIO E DEFINITIVO:

6.2.1. A CONTRATANTE efetuará o recebimento do objeto contratado, provisoriamente, para efeito de posterior verificação da conformidade do objeto com a especificação, e definitivamente, após a verificação da qualidade e quantidade do objeto e consequente aceitação.

6.2.2. Em caso de rejeição total/parcial do objeto contratado, correção, substituição ou demais hipóteses de descumprimento de outras obrigações contratuais, avaliadas na etapa de recebimento, sujeitará a CONTRATADA à aplicação das sanções administrativas cabíveis.

6.2.3. Os bens poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes no Termo de Referência e na proposta, devendo ser substituídos no prazo de 15 (quinze) dias corridos, a contar da notificação da CONTRATADA, às suas custas, sem prejuízo da aplicação das penalidades.

6.3. TERMO DE RECEBIMENTO PROVISÓRIO:

6.3.1. O CONTRATANTE receberá provisoriamente o objeto contratado, mediante emissão de termo circunstanciado assinado pelas partes, em até 5 (cinco) dias após a entrega do objeto.

6.3.2. O recebimento provisório caberá ao agente fiscalizador especialmente designado para acompanhamento e fiscalização do contrato decorrente desta proposição.

6.3.3. A fiscalização do contrato procederá a observação da qualidade do objeto, registrando a data de entrega dos materiais e a data de emissão do termo de recebimento provisório, bem como anotará quaisquer ocorrências que impactem na avaliação da qualidade do fornecimento pela CONTRATADA.

6.4. TERMO DE RECEBIMENTO DEFINITIVO:

6.4.1. Os representantes da administração deverão conferir a qualidade e especificações funcionais dos equipamentos entregues e confrontá-las com as exigências editalícias, promoverem testes de desempenho (se for o caso), verificar licenças, registrar a data de entrega, emitir o recibo e o termo de recebimento definitivo, bem como registrar quaisquer ocorrências que impactem na avaliação da qualidade do fornecimento pela CONTRATADA.

6.4.2. O recebimento definitivo caberá ao agente fiscalizador especialmente designado para acompanhamento e fiscalização do contrato decorrente desta proposição.

6.4.3. O objeto contratado será rejeitado caso esteja em desacordo com as especificações constantes do Termo de Referência, devendo a CONTRATANTE apontar por escrito esta ocorrência, onde detalhou as razões para deixar de emitir o termo de recebimento definitivo e indicará as falhas e pendências verificadas.

6.4.4. O recebimento definitivo do objeto não exclui nem reduz a responsabilidade da CONTRATADA com relação ao funcionamento e configuração divergente do especificado, durante todo o seu período de garantia.

6.4.5. Ficam designados para compor a comissão que efetuará o recebimento definitivo o agente fiscalizador e o gestor do contrato, bem como seus respectivos substitutos.

CLÁUSULA SÉTIMA – DO VALOR E DO PAGAMENTO

7.1. O valor global do contrato é de R\$ _____ (_____), conforme abaixo discriminado:

GRUPO 1 - SOLUÇÃO DE WEB APPLICATION FIREWALL (WAF)						
ITEM	DESCRIÇÃO	CATMAT/ CATSER	UNIDADE DE MEDIDA	QUANT.	VALOR UNITÁRIO	VALOR TOTAL
1	FORNECIMENTO DE SOLUÇÃO DE WEB APPLICATION FIREWALL(WAF), DO TIPO APPLIANCE VIRTUAL, COM GARANTIA DE 60(SESENTA) MESES.	27464	UN		R\$	R\$
2	FORNECIMENTO DE SOLUÇÃO DE WEB APPLICATION FIREWALL(WAF), DO TIPO APPLIANCE FÍSICO, COM GARANTIA DE 60(SESENTA) MESES.	27472	UN		R\$	R\$
3	CAPACIDADE ADICIONAL PARA SOLUÇÃO EM FIREWALL DE APLICAÇÕES WEB	27464	UN		R\$	R\$
4	SERVIÇO DE INSTALAÇÃO E REPASSE DE CONHECIMENTO HANDS-ON	27324	UN		R\$	R\$
5	TREINAMENTO ESPECIALIZADO	27260	UN		R\$	R\$
6	SERVIÇO DE OPERAÇÃO ASSISTIDA	27324	UN		R\$	R\$
VALOR TOTAL						R\$

7.2. O pagamento será efetuado através de Ordem Bancária, mediante depósito na conta-corrente da CONTRATADA, até o 10º (décimo) dia útil da data da liquidação da despesa, observado o estabelecido no art. 5º da Lei nº 8.666/93, e desde que não ocorra fator impeditivo provocado pela CONTRATADA.

7.2.1. Em caso de apresentação de Nota Fiscal/Fatura contendo código de barras, o pagamento será efetuado por meio de Ordem Bancária de Fatura, devendo-se observar a emissão do documento pelo valor líquido, não sendo dispensada a indicação do valor bruto e do valor da retenção tributária.

7.2.2. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária de pagamento.

7.2.3. No caso do valor do pagamento não ultrapassar o limite de que trata o inciso II do art. 24, da Lei nº 8.666/93, o mesmo deverá ser efetuado no prazo de até 5 (cinco) dias úteis, nas condições referidas no item 7.2.

7.3. Nesta contratação não será aplicado o Instrumento de Medição de Resultado (substituto do Acordo de Nível de Serviço – ANS).

7.4. Para fazer jus ao pagamento, a CONTRATADA deverá apresentar Nota Fiscal/Fatura discriminando os bens/serviços efetivamente fornecidos/prestados.

7.4.1. Se optante pelo Simples Nacional, deverá ser apresentada a declaração de que trata o art. 6º da Instrução Normativa nº 1234/2012, em meio físico ou eletrônico assinado por certificação digital (não será aceito simples cópia digitalizada).

7.4.2. No caso de contrato de prestação de serviços continuados, a declaração será apresentada por ocasião do 1º (primeiro) pagamento, sendo dispensada nos demais. Caso haja a prorrogação do contrato, a declaração deverá ser apresentada novamente no 1º (primeiro) pagamento do novo período de vigência.

7.5. Nenhum pagamento será efetuado à CONTRATADA enquanto pendente de liquidação qualquer obrigação financeira que lhe for imposta, em virtude de penalidade ou inadimplência, sem que isso gere direito ao pleito de reajustamento de preços ou correção monetária.

7.6. Os pagamentos serão realizados após a comprovação da regularidade fiscal e trabalhista exigidas na habilitação, mediante a consulta *on-line* junto ao Sistema de Cadastramento Unificado de Fornecedor – SICAF.

7.7. Constatada a situação de irregularidade fiscal e trabalhista da CONTRATADA, será providenciada a sua advertência, por escrito, no sentido de que, no prazo de cinco (05) dias úteis, a contratada regularize sua situação ou, no mesmo prazo, apresente sua defesa.

7.8. O prazo do item anterior poderá ser prorrogado uma vez, por igual período, a critério da CONTRATANTE.

7.9. Não havendo regularização ou sendo a defesa considerada improcedente, a CONTRATANTE comunicará os órgãos responsáveis pela fiscalização da regularidade fiscal e trabalhista quanto à inadimplência da CONTRATADA, bem como quanto à existência de pagamento a ser efetuado pela CONTRATANTE, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

7.10. Persistindo a irregularidade, a CONTRATANTE deverá adotar as medidas necessárias à rescisão do contrato, assegurada à CONTRATADA a ampla defesa.

7.11. Havendo a efetiva prestação de serviços ou o fornecimento dos bens, os pagamentos serão realizados normalmente, até que se decida pela rescisão contratual, caso a CONTRATADA não regularize sua situação.

7.12. Somente por motivo de economicidade, segurança nacional ou outro interesse público de alta relevância, devidamente justificado, em qualquer caso, pelo Diretor(a)-Geral, não será rescindido o contrato em execução com a CONTRATADA inadimplente.

7.13. Pela prestação do serviço, serão efetuadas as seguintes retenções:

7.13.1. Tributos e contribuições federais (IR, CSLL, PIS e COFINS) previstos no artigo 64 da Lei nº 9.430, de 27.12.96, e [Instrução Normativa RFB nº 1.234](#), de 11.01.12, enquadrando os itens 1 e 3 a 6 no código 6190 (Demais serviços) e o item 2 no código 6147 (Mercadorias e bens em geral) da Tabela de Retenção do Anexo I da referida Instrução Normativa, exceto quando se tratar de empresa optante pelo simples nacional, hipótese em que deverá ser apresentada, no ato da assinatura do contrato, a declaração prevista no Anexo IV da mesma Instrução Normativa; e

7.13.2. Imposto Sobre Serviços (ISS) previsto na [Lei Complementar nº 116](#), de 31.07.03, enquadrando os licenciamentos da solução (itens 1 e 3) no item 1.05 da Lista de Serviços anexa à referida Lei, os serviços de instalação e de operação assistida (itens 4 e 6) no item 1.07 e o treinamento (item 5) no item 8.02 da mesma Lista. Para efeito do disposto neste tópico será observado o contido nos artigos 3º e 4º da Lei Complementar nº 116/2003 (local do estabelecimento

prestador). Em se tratando de empresa optante pelo simples nacional, a retenção se dará conforme enquadramento no respectivo Anexo da [Lei Complementar nº 123/2006](#).

7.13.3. A empresa deverá destacar no documento fiscal as alíquotas dos tributos e das contribuições, bem como os correspondentes valores, nos termos das respectivas legislações. Em caso de descumprimento desta determinação, a empresa sofrerá a retenção pelas alíquotas máximas previstas.

7.13.4. Na hipótese de ocorrer alteração em alguma das normas referenciadas neste item, será aplicada a retenção correspondente prevista na legislação em vigor.

7.14. Nos casos de eventuais atrasos de pagamento, desde que a CONTRATADA não tenha concorrido de alguma forma para tanto, fica convencionado que a taxa de atualização financeira devida pela CONTRATANTE, entre a data acima referida e a correspondente ao efetivo adimplemento da parcela, será calculada mediante a aplicação da seguinte 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 a ser paga; e

I = Índice de atualização financeira = 0,0001644, assim apurado:

$$I = (TX/100)/365$$

$$I = (6/100)/365$$

$$I = 0,0001644$$

TX = Percentual da taxa anual = 6%

7.15. As notas fiscais apresentadas em desacordo com o estabelecido no contrato ou com qualquer vício serão devolvidas à CONTRATADA, não correndo, neste caso, o prazo estipulado no item 7.2, iniciando-se, somente, a partir da sua completa regularização.

7.16. No primeiro e no último mês de vigência contratual, os valores serão rateados à base de 1/30 (um trinta avos) por dia do valor mensal dos serviços, considerando-se o mês de 30 (trinta) dias. Nos meses intermediários os encargos da efetiva prestação dos serviços serão cobrados considerando-se o mês de 30 (trinta) dias, para que não ultrapasse o valor global (quando aplicável).

CLÁUSULA OITAVA – DA DOTAÇÃO ORÇAMENTÁRIA

8.1. A despesa com a execução do presente contrato correrá à conta de recursos previstos no Orçamento da Justiça Eleitoral, na Ação: _____ - PTRES _____, Natureza de Despesa —_____.

8.2. Para cobertura da despesa foi emitida a Nota de Empenho no 202__NE_____, de ___/___/20___, à conta da dotação especificada nesta cláusula.

CLÁUSULA NONA - PRAZO DE VIGÊNCIA

9.1. O presente contrato terá vigência de 120 (cento e vinte) dias, com início a partir de sua assinatura, com eficácia após a publicação do seu extrato no Diário Oficial da União, a permitir o recebimento e pagamento do objeto, não sendo, porém, prejudicada a garantia prevista no item 6.1 da a Cláusula Sexta.

CLÁUSULA DÉCIMA – DO REAJUSTE

10.1. Os preços inicialmente contratados são fixos e irredutíveis no prazo de 12 (doze) meses, contado da data limite para apresentação da proposta comercial que fundamentou a contratação.

10.2. Após o prazo de 12 (doze) meses, contado da data limite para apresentação da proposta, os preços poderão ser reajustados, utilizando-se a variação do Índice de Custo da Tecnologia da Informação (ICTI) ou outro que venha a substituí-lo. Os demais e sucessivos reajustes deverão, também, respeitar o interregno de 12 (doze) meses da data de início dos efeitos financeiros do último reajuste ocorrido.

10.3. O reajuste previsto nesta cláusula será calculado com base no índice acumulado dos últimos 12 (doze) meses contados da data da apresentação da proposta ou do mês subsequente ao último reajuste concedido, aplicado exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

10.4. Os reajustes deverão ser obrigatoriamente precedidos de solicitação da CONTRATADA.

10.5. Caso a CONTRATADA não solicite tempestivamente o reajuste e o contrato seja prorrogado sem pleiteá-lo, ocorrerá a preclusão do direito ao reajuste.

10.6. Também ocorrerá a preclusão do direito ao reajuste se o pedido for formulado depois de extinto o contrato.

10.7. O reajuste terá seus efeitos financeiros iniciados a partir da data de aquisição do direito da CONTRATADA, nos termos do item 10.2 acima.

CLÁUSULA DÉCIMA PRIMEIRA – DA ALTERAÇÃO

11.1. Este instrumento poderá ser alterado na ocorrência de quaisquer dos fatos estipulados no art. 65 da Lei n.º 8.666/93.

CLÁUSULA DÉCIMA SEGUNDA – DAS SANÇÕES ADMINISTRATIVAS E RECURSOS

12.1. Ficará impedida de licitar e de contratar com a União e será descredenciada no SICAF, pelo prazo de até cinco anos, sem prejuízo das multas previstas em edital e no contrato e das demais cominações legais, garantido o direito à ampla defesa, a CONTRATADA que, convocada dentro do prazo de validade de sua proposta:

- a) Deixar de entregar a documentação exigida no Edital;
- b) Não assinar a Ata de Registro de Preços ou o contrato e/ou não receber a Ordem de Fornecimento e/ou de Serviço;
- c) Apresentar documento falso ou fizer declaração falsa;
- d) Causar atraso na execução do objeto do contrato;
- e) Não mantiver a proposta, injustificadamente;
- f) Falhar ou fraudar na execução do contrato;
- g) Comportar-se de modo inidôneo;
- h) Cometer fraude fiscal.

12.2. Sem prejuízo das demais sanções previstas no art. 87 da Lei nº 8.666/93, pelo atraso injustificado e inexecução total ou parcial do contrato, a Administração do Tribunal Regional Eleitoral do Pará, poderá, garantida a defesa prévia, aplicar à CONTRATADA as seguintes sanções:

- a) Advertência, nas hipóteses de faltas leves, assim entendidas aquelas que não acarretem prejuízos para o TRE/PA;
- b) Multa compensatória de até 10% (dez por cento) sobre o valor global da Ata de Registro de Preços, na hipótese de recusa em assinar a Ata de Registro de Preços ou do contrato, na hipótese de recusa em assinar o instrumento de contrato;
- c) Multa compensatória de até 10% (dez por cento) sobre o valor global do respectivo material, na hipótese de recusa em receber a Ordem de Fornecimento e/ou de Serviço;
- d) Multa compensatória de até 10% (dez por cento) sobre o valor global do respectivo material, na hipótese de inexecução parcial ou total da obrigação.

12.3. Pelo atraso injustificado na execução do contrato, a CONTRATANTE deverá, garantida a defesa prévia, aplicar à CONTRATADA multa moratória de 0,2% (dois décimos por cento) por dia de atraso na entrega do material e/ou conclusão do serviço contratado, tomando por base o valor global do respectivo material, limitado a 10% (dez por cento).

12.4. O atraso injustificado na execução do contrato por período superior a 30 (trinta) dias, bem como deixar de manter todas as condições de habilitação, poderá ensejar a rescisão do contrato.

12.5. As multas aplicadas serão descontadas dos créditos da CONTRATADA ou, na impossibilidade, recolhidas no prazo de até 15 (quinze) dias, a contar da data da comunicação oficial para pagamento. Em caso de não recolhimento, o valor será cobrado judicialmente, consoante o disposto no § 3º do art. 86 e § 1º do art. 87 da Lei n.º 8.666/93, acrescida de juros moratórios de 0,5% (meio por cento) ao mês e correção monetária pelo Índice de Preços ao Consumidor Amplo Especial – IPCA-E, nos termos art. 27 da Lei n.º 9.069/95, c/c o art. 3º da Lei n.º 10.192/2001.

12.6. Os prazos de adimplemento das obrigações contratadas admitem prorrogação nos casos e condições especificados no §1º do art. 57 da Lei 8.666/93, e a solicitação dilatória deverá ser recebida contemporaneamente ao fato que a ensejar.

12.6.1. O pedido de prorrogação do prazo de execução não terá efeito suspensivo e deverá ser encaminhado por escrito, antes de expirado o prazo contratual, anexando-se documento comprobatório do alegado pela CONTRATADA, competindo ao(à) Secretário(a) de Administração a concessão da prorrogação pleiteada.

12.7. Compete ao Diretor-Geral a apreciação e aplicação das penalidades previstas nesta Cláusula, facultada a defesa do interessado, no prazo de 05 (cinco) dias úteis, contados da sua notificação.

12.8. Da aplicação das penalidades previstas nesta Cláusula caberá recurso, no prazo de 05 (cinco) dias úteis, contados da notificação, que será dirigido à autoridade superior, por intermédio da que praticou o ato, a qual poderá reconsiderar a sua decisão, ou, fazê-lo subir devidamente informado.

12.9. As sanções de multa poderão ser aplicadas juntamente com as demais penalidades previstas.

12.10. As penalidades aplicadas serão obrigatoriamente registradas no SICAF.

CLÁUSULA DÉCIMA TERCEIRA - DA SUBCONTRATAÇÃO

13.1. É vedada a subcontratação do objeto deste contrato.

CLÁUSULA DÉCIMA QUARTA - DA GARANTIA

14.1. Não será exigida garantia contratual para este contrato.

CLÁUSULA DÉCIMA QUINTA - DA RESCISÃO

15.1. Poderá ser rescindido o presente contrato, caso ocorram os motivos constantes dos artigos 77, 78 e 79 da Lei n.º 8.666/93, mediante formalização, assegurado o contraditório e a ampla defesa.

CLÁUSULA DÉCIMA SEXTA – DA PUBLICIDADE

16.1. O extrato do presente contrato será publicado no Diário Oficial da União, conforme o disposto no art. 20 do Anexo I do Decreto n.º 3.555/2000, correndo as despesas por conta da CONTRATANTE.

CLÁUSULA DÉCIMA SÉTIMA – DOS CASOS OMISSOS

17.1. Fica estabelecido que, caso venha a ocorrer algum fato não previsto neste instrumento - os chamados casos omissos, estes deverão ser resolvidos entre as partes contratantes, respeitados o objeto deste instrumento, a legislação e as demais normas reguladoras da matéria, em especial a Lei n.º 8.666/93, aplicando-lhe, quando for o caso, supletivamente, os princípios da Teoria Geral dos Contratos e as disposições do Direito Privado.

CLÁUSULA DÉCIMA OITAVA – DO FORO

18.1 As controvérsias decorrentes deste contrato serão dirimidas no foro da Seção Judiciária de Belém, Capital do Estado do Pará, pela Justiça Federal, nos termos do art. 109, I, da Constituição Federal.

E por estar, assim, justo e avençado, depois de lido e achado conforme, foi o presente contrato lavrado, assinado e datado eletronicamente pelas partes.

(assinado e datado eletronicamente)

CONTRATANTE

(assinado e datado eletronicamente)

CONTRATADA



Documento assinado eletronicamente por **DILSON ATHIAS MESQUITA, Pregoeiro**, em 11/07/2022, às 14:17, conforme art. 1º, III, "b", da Lei 11.419/2006.



A autenticidade do documento pode ser conferida no site https://sei.tre-pa.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1617808** e o código CRC **B9347458**.