TRIBUNAL REGIONAL ELEITORAL DE MATO GROSSO
Av. Historiador Rubens de Mendonça, 4750 - Bairro Centro Político e Administrativo - CEP 78049-941 - Cuiabá - MT - http://www.tre-mt.jus.br/

TERMO DE REFERÊNCIA Nº 0323949/2021

TRIBUNAL REGIONAL ELEITORAL DE MATO GROSSO

SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

TERMO DE REFERÊNCIA

1. INTRODUÇÃO

1.1. Nos termos da Lei nº 10.520/02, do Decreto nº 10.024/2019 e da Lei nº 8.666/93, e suas alterações, bem como da Resolução n. 23.234/2010-TSE, da Resolução nº 182/2013/CNJ e da Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019, apresentamos o presente Termo de Referência com a finalidade de subsidiar a administração desta Corte na 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, BEM COMO CAPACITAÇÃO DE PESSOAL.**

1.2. Neste instrumento estão descritas as condições para determinar os elementos necessários e suficientes para caracterizar o objeto da licitação, assegurando a viabilidade técnica, a avaliação do custo de manutenção, a definição de métodos e prazos de entrega e recebimento, bem como orientar a execução e a fiscalização do contrato.

1.3. Os serviços definidos neste documento estão de acordo com os padrões de desempenho e qualidade usuais de mercado e, portanto, enquadram-se como serviços comuns para fins do disposto no Decreto nº 5.450/05, conforme os documentos de análise da contratação juntados no processo administrativo que formaliza está aquisição.

1.4. CONCEITUAÇÃO

a) GESTOR DO CONTRATO / FISCAL DO CONTRATO / COMISSÃO DE FISCALIZAÇÃO – servidor(es) especialmente designado(s) para exercer o acompanhamento e a fiscalização da execução contratual;

b) ORDEM DE SERVIÇO - documento utilizado pela Administração para a solicitação, o acompanhamento e o controle de tarefas relativas à execução dos contratos, podendo ser substituída pela nota de empenho;

c) SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO/STI – unidade administrativa do Tribunal, responsável pela área de TIC.

d) COORDENADORIA DE INFRAESTRUTURA COMPUTACIONAL/CIEC - unidade administrativa do Tribunal responsável pela área de infraestrutura de TIC.

e) SEÇÃO DE GERENCIA DE REDES/SGR – unidade administrativa do Tribunal responsável pela área de conectividade.

f) CHAMADO TÉCNICO – Pedido de suporte, de reparo ou de informação sobre equipamentos ou softwares.

g) VALOR TOTAL DA CONTRATAÇÃO – Valor de todas as aquisições/contratações resultantes desta licitação, contratado com determinada empresa.

2. DO OBJETO

2.1. A presente licitação tem por objeto a 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, bem como capacitação de pessoal.

3. DA JUSTIFICATIVA

3.1. DA NECESSIDADE DA AQUISIÇÃO

3.1.1.A partir de ampliação da disponibilização das soluções de software baseadas nos protocolos que constituem a Web, principalmente, HTTP (*HyperText Transfer Protocol*) e HTTPS (*HyperText Transfer Protocol Secure*) para acessos externos e internos, respectivamente, via Internet e Intranet, tornou-se necessário reduzir a superfície de ataque, ampliando a segurança da informação deste TRE-MT, uma vez que tais aplicações são vetores potenciais para exploração de falhas, principalmente ao se considerar a complexidade das arquiteturas de softwares e plataformas utilizadas.

3.1.2.Nesse cenário, para identificar e evitar ataques destinados a explorar recursos de camada de aplicação, considerando o modelo de referência *Open System Interconnection* definido pela *International Organization for Standardization* (ISO/OSI), são necessárias ferramentas especializadas como as soluções WAF com suporte de segurança a APIs (*Application Program Interfaces*).

3.1.3.Adicionalmente, considerando a necessidade de escalabilidade das aplicações, bem como o crescente uso de soluções de software baseadas em contêineres e Micro Serviços, torna-se necessário que a solução pretendida inclua solução de balanceamento de carga, visando equalizar a distribuição de carga de acessos aos sistemas, tanto em ambiente interno quanto externo, nos diversos servidores de aplicação disponíveis na infraestrutura do TRE-MT, garantindo os requisitos necessário de desempenho e disponibilidade, principalmente, para sistemas críticos.

3.1.4.Destaca-se, também, que nos últimos anos, tem se formalizado acordos de nível de serviço impostos à área de TIC que determinam a alta disponibilidade, bem como a preservação dos ativos institucionais, das informações dos usuários e dos dados dos cidadãos. A inexistência de uma solução de segurança da informação atualizada agride tais recomendações e põe em risco a credibilidade da instituição em caso de acessos não autorizados. Além disso, a Lei Geral de Proteção de Dados (LGPD, Lei nº 13.709, de 14 de agosto de 2018) obriga às instituições a possuírem mecanismos de proteção aptos a fazer frente às possíveis ameaças.

3.2. DOS OBJETIVOS

3.2.1.Atuação Institucional: Garantir a disponibilidade de informação ao público externo;

3.2.2.Eficiência Operacional: Garantir a comunicação, por meio eletrônico, das comunicações judiciais;

3.2.3.Infraestrutura e Segurança da Informação: Garantir a eficiência da infraestrutura lógica e ampliar a segurança da informação considerando às atividades administrativas e judiciais, inclusive de forma remota (teletrabalho).

3.3. DA JUSTIFICATIVA PARA AGRUPAMENTO DE ITENS EM LOTE ÚNICO

3.3.1. O agrupamento em lote único se faz necessário, pois, trata-se de aquisição de solução composta de hardware, software e subscrição para atualizações, suporte e garantia, de fabricante único, visando estabelecer um cluster de alta disponibilidade.

3.3.2. Nesse cenário, destaca-se que a implantação dos equipamentos na infraestrutura do TRE-MT, bem como o estabelecimento da configuração inicial deverá ser realizada por empresa especializada na

tecnologia dos *appliances* a serem adquiridos, eliminando, assim, a possibilidade de separação em lote distinto, uma vez que, obrigatoriamente, a vencedora do item 2 (dois) deverá implantar e configurar, com profissionais especializados, a solução a ser adequirida no item 1.

3.3.3. O mesmo cenário se repete em relação às capacitações, uma vez que se destinam a qualificar a equipe técnica deste TRE-MT na solução a ser adquirida, bem como nas funcionalidades licenciadas, inviabilizando, assim, a separação em lote distinto.

3.3.4. Assim, ao optar pelo agrupamento em lote único, visa-se mitigar o risco de aquisição de itens não vinculados a solução adquirida no item 1 (um), uma vez que não é possível, em múltiplos lotes, vincular os treinamentos e serviços de instalação e configuração ao fabricante da solução prevista no item 1 (um).

4.DA SOLUÇÃO E SERVIÇOS A SEREM CONTRATADOS (LOTE ÚNICO).

4.1. A solução a ser adquirida se encontra especificada em 3 (três) itens, conforme tabela 1.

ITEM	QTD.	CATMAT/ CATSER	PRODUTO	DESCRIÇÃO
1	2	27464	*Solução de* Web Application Firewall e balanceamento de carga	Appliances físicos redundantes, novos e não remanufaturados, constantes da linha de produção atual do fabricante, com funcionalidades de *Web Application Firewall* e balanceador de carga.
2	1	27324	Serviço de instalação e configuração da solução de *Web Application firewall* e balanceamento de carga	Serviço de instalação física na infraestrutura de TIC do TRE-MT e configuração das funcionalidades contratadas.
3	4	27260	Capacitação	Capacitação individual, incluindo conceitos de configuração e operação da solução contratada, bem como das funcionalidades de Web Application Firewall e balanceamento de carga.

Tabela 1. Relação de itens que compõem a solução

4.2. Considerando que a solução deverá operar em *cluster,* observa-se que o quantitativo a indicado no item 1 da tabela 1, reflete a configuração mínima necessária, assim como o item 2, uma vez que trata-se da implantação inicial da solução;

4.3. Em relação ao item 3, destaca-se que deverão ser treinados 2 (dois) servidores da seção de Gerência de Redes, 1 (um) servidor da área de Infraestrutura de TIC e o Gestor de Segurança da Informação, totalizando, assim, 4 (quatro) capacitações.

5. DAS CONDIÇÕES DE SIGILO

5.1. A empresa a ser contratada será a responsável pela segurança das informações, as quais eventualmente terá acesso em virtude da prestação dos serviços;

5.2. Qualquer divulgação de informação sigilosa ou considerada sigilosa pelo Tribunal representará quebra de sigilo que ensejará a quebra de contrato e estará sujeita a multa de 10% (dez por cento) do valor total da contratação, assegurando-se ainda ao servidor ofendido (servidor funcionário ou prestador de serviço em qualquer condição), o direito de reparação quanto a danos morais, materiais e lucros cessantes;

5.2.1. A punição de natureza pecuniária poderá ser aplicada mesmo no caso de a administração decidir pela continuidade do contrato;

5.2.2. A criação de acesso, alteração de senhas ou permissões sem consentimento expresso da equipe técnica do Tribunal, bem como as condutas similares, constituir-se-ão violações de segurança e ensejarão as mesmas sanções que a divulgação de informação sigilosa;

5.3. A princípio, toda e qualquer informação disponível nas instalações do Tribunal, dos Cartórios Eleitorais e das Unidades de Atendimento, bem como as acessórias - as quais as contratadas venham a ter acesso em virtude da execução dos serviços (*on site* ou remotos) –, são classificadas como sigilosas pelo TRE-MT. Salvo disposição em contrário por esta Corte, endereçada à empresa contratada, sua divulgação ensejará quebra de sigilo;

5.4. É responsabilidade exclusiva da Contratada a manutenção do sigilo das informações por parte de seus funcionários, inclusive aqueles que não mais pertençam ao seu quadro de pessoal.

6. DAS OBRIGAÇÕES DA CONTRATADA

6.1. Entregar os equipamentos de acordo com as especificações contidas neste termo de referência, responsabilizando-se pela troca, no prazo máximo de 15 (quinze) dias, daqueles que, porventura, estejam fora das especificações ou danificados, independentemente do motivo alegado;

6.2. Disponibilizar os treinamentos na forma deste Termo de Referência e assegurar a qualidade da instrutória e do conteúdo ministrado;

6.3. Informar os procedimentos e dados que serão necessários para abertura e registro de chamados técnicos para a prestação da assistência técnica no momento da proposta ou da assinatura do contrato;

6.4. Lançar os códigos dos serviços relativos à contratação no site da fabricante;

6.5. Atender e responder os questionamentos técnicos do Tribunal relativos à Solução durante toda a vigência do contrato;

6.6. Atender os chamados técnicos dentro do que determina o ANS.

6.7. Arcar com a responsabilidade de troca ou reparo dos equipamentos que apresentarem defeito, vício ou mal funcionamento durante todo o período da contratação e da garantia;

6.8. Em caso de necessidade de assistência técnica fora da Sede do Tribunal, devidamente autorizada pelo FISCAL DO CONTRATO, arcar com as providências e despesas de envio e recebimento dos equipamentos que vierem a apresentar problemas de funcionamento durante o período da contratação do serviço de suporte técnico;

6.9. Responder pelo cumprimento total do contrato e eventuais obrigações acessórias perante o Tribunal (União);

6.10. Informar ao TRE-MT pelo menos um contato de e-mail por meio do qual serão mantidos os contatos oficiais.

6.11. Constituem, também, obrigações da(s) empresa(s) contratada(s):

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

6.11.2. Utilizar melhores práticas, capacidade técnica, materiais, equipamentos, recursos humanos e supervisão técnica e administrativa, para garantir a qualidade dos serviços e o atendimento às especificações contidas no Contrato, Edital e em seus Anexos;

6.11.3. Reportar formal e imediatamente à fiscalização quaisquer problemas, anormalidades, erros e irregularidades que possam comprometer a execução do objeto;

6.11.4. Responder integralmente por quaisquer perdas ou danos causados ao Tribunal ou a terceiros em razão de ação ou omissão, dolosa ou culposa, sua ou dos seus profissionais ou de quaisquer pessoas agindo a seu mando em razão da execução do objeto, independentemente de outras cominações contratuais ou legais a que estiver sujeito;

6.11.5. Cumprir e garantir que seus profissionais estejam cientes, aderentes e obedeçam rigorosamente às normas e aos procedimentos estabelecidos na Política de Segurança da Informação do Tribunal;

6.11.6. Manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de que tomar conhecimento em razão da execução do objeto do Contrato, respeitando todos os critérios de sigilo, segurança e inviolabilidade, aplicáveis aos dados, informações, regras de negócio, documentos, entre outros, na forma do item “DAS CONDIÇÕES DE SIGILO” deste documento, bem como as boas práticas reconhecidas pelo mercado;

6.11.7. Substituir por outro profissional de qualificação igual ou superior qualquer um dos seus profissionais cuja qualificação, atuação, permanência ou comportamento decorrentes da execução do objeto forem julgados prejudiciais, inconvenientes ou insatisfatórios à disciplina do órgão ou ao interesse do serviço público, sempre que exigido pela fiscalização;

6.11.8. Manter seus profissionais nas dependências do Tribunal adequadamente trajados e identificados com uso permanente de crachá, com foto e nome visível;

6.11.9. Apresentar as notas fiscais, contendo a discriminação exata dos bens e serviços contratados (prazos de execução, quantidades e valores contratados), junto com os relatórios apropriados;

6.11.10. No caso do fornecimento de equipamento e/ou materiais, comprovar a origem dos bens importados oferecidos e a quitação dos tributos de importação a eles referentes, que deve ser apresentada no momento da entrega do objeto.

7. OBRIGAÇÕES DO TRE-MT

7.1. Recusar os serviços executados, os equipamentos ou os *softwares* que não atenderem as especificações estabelecidas neste Termo de Referência, anotando o fato, como descumprimento parcial do contrato;

7.2. Além das obrigações resultantes da observância da legislação pertinente, são também obrigações do TRE-MT:

7.2.1. Efetuar os pagamentos devido, de acordo com o estabelecido neste documento e no contrato;

7.2.2. Proporcionar todas as facilidades para que a Contratada possa desempenhar seus serviços dentro das normas deste Termo de Referência e do Contrato, dos documentos que o acompanham e da legislação pertinente, além das boas práticas de mercado;

7.2.3. Exercer a fiscalização dos serviços por servidores especialmente designados, na forma prevista na Lei nº 8666/93;

7.2.4. Não permitir que a mão de obra execute tarefas em desacordo com as preestabelecidas deste Termo de Referência e no Contrato;

7.2.5. Manifestar-se formalmente em todos os atos relativos à execução do contrato, em especial, aplicação de sanções, alterações e repactuações do contrato;

7.2.6. Comunicar quaisquer irregularidades observadas na execução dos serviços contratados à Contratada, manifestando-se formalmente em todos os atos representativos relativos à execução do contrato;

7.2.7. Anotar as ocorrências relacionadas com a execução dos serviços contratados, determinando, no que julgar necessário, à regularização das faltas e defeitos observados;

7.2.8. Aplicar à Contratada, penalidades por descumprimento deste Termo de Referência e de cláusulas contratuais;

7.3. A empresa contratada poderá formalizar as comunicações por e-mail, principalmente à fiscalização do contrato por meio dos e-mails sgr@tre-mt.jus.br e ciec@tre-mt.jus.br.

8. DA ENTREGA DOS EQUIPAMENTOS

8.1. Os equipamentos deverão ser entregues em um prazo máximo de 60 (sessenta) dias, devidamente licenciados, a contar da data de recebimento da nota de empenho ou assinatura do contrato;

8.1.1. A não entrega no prazo especificado, ou o atraso na substituição daqueles divergentes das especificações deste Termo de Referência ou em mau funcionamento, ensejara a sanção de multa na ordem de 0,5% (meio por cento) sobre o valor do ITEM contratado (ITEM 1), limitada a 10 % do valor total da contratação, por dia de descumprimento.

8.2. Os equipamentos deverão ser entregues em horário de expediente, na Seção de Patrimônio na sede deste Tribunal, situado na Avenida Historiador Rubens de Mendonça n.º 4750, Bosque da Saúde, Cuiabá –

MT, acompanhados concomitantemente da correspondente nota fiscal e certificados de garantia (se aplicável);

8.3. A nota fiscal deverá, a cada entrega, ser preenchida de acordo com as especificações apresentadas na nota de empenho respectiva e conter as informações bancárias para quitação;

8.4. Eventual pedido da Contratada para substituição de modelo/marca de equipamento não suspenderá o prazo de entrega;

8.5. O pedido de substituição de equipamento que não implique ônus à administração do Tribunal, bem como daqueles que se tratarem de substituição de equipamento obsoleto (fora de mercado), poderá ser autorizado pela Fiscalização mediante aceite do Secretário da STI;

8.6. O processo de pagamento e recebimento dos equipamentos poderá ser realizado separado dos demais itens descritos neste Termo de Referência.

9. DA ENTREGA DOS SERVIÇOS DE SUBSCRIÇÃO

9.1. Após a assinatura do contrato, a Licitante vencedora do certame deverá efetuar o lançamento das licenças na conta do TRE-MT no site, ou solução específica, da empresa fabricante da solução no prazo máximo de 30 (trinta) dias (RECEBIMENTO PROVISÓRIO). Isso feito, o Gestor do Contrato deverá certificar o recebimento (RECEBIMENTO DEFINITIVO), no prazo de 15 (quinze) dias.

9.2. Concluído o recebimento, a nota fiscal poderá ser encaminha para a fiscalização para atestação e pagamento. Ela deverá ser preenchida de acordo com as especificações apresentadas na nota de empenho respectiva e conter as informações bancárias para quitação.

9.3. Sustentabilidade ambiental: Não serão aceitas mídias para os softwares ou manuais impressos.

10. DA ENTREGA DA INSTALAÇÃO (ITEM 2)

10.1. Após a emissão do aceite da instalação e, também, da finalização do repasse de conhecimento, previsto no item 6, a equipe técnica da Secretaria de Tecnologia da Informação do TRE-MT terá 5 (cinco) dias úteis para emitir o laudo de avaliação técnica.

10.1.1. Após a emissão do laudo, a nota fiscal poderá ser encaminhada para a fiscalização para atestação e pagamento. Ela deverá ser preenchida de acordo com as especificações apresentadas na nota de empenho respectiva e conter as informações bancárias para quitação.

11. DA ENTREGA DAS CAPACITAÇÕES (ITEM 3)

11.1. Quanto aos treinamentos, não serão aceitos os não oficiais ou cujo conteúdo ministrado não abranja a utilização da solução para o fim a que se destina, bem ainda, aqueles cujos certificados não forem emitidos no prazo máximo de 15 (quinze) dias contados da conclusão da capacitação;

11.1.1. Não serão aceitos, também, treinamentos ministrados por instrutor que não demonstrar o necessário conhecimento prático sobre o conteúdo do curso e sobre a Solução contratada;

11.1.2. A não aceitação da capacitação implicará no não pagamento dos serviços realizados.

11.2. A empresa a ser contratada deverá emitir certificados de participação contendo a exata carga horária do treinamento e a participação do discente;

11.2.1. Os Treinamentos poderão ser customizados de modo a melhor atenderem às necessidades do TRE-MT mediante acordo prévio com a fiscalização do contrato desde que esteja contido o conteúdo mínimo recomendado pela Fabricante.

11.3. O treinamento será considerado entregue após sua realização e emissão dos certificados digitais e deverá ser ministrado em um prazo máximo de 180 (cento e oitenta) dias a contar do recebimento da nota de empenho, se outra data não for solicitada pela fiscalização;

11.4. No caso de não cumprimento das condições do Treinamento, quer pela qualidade do curso, quer pela qualidade do material ou equipamentos colocados à disposição, ou por qualquer divergência no objeto

desta contratação, a empresa a ser contratada deverá repeti-lo sob suas expensas, responsabilizando-se pelo deslocamento do pessoal e pagamento de diárias na forma e valores dispendidos pelo Tribunal, aos servidores em data a ser estipulada pelo Fiscal do Contrato, sob pena de descumprimento total da contratação com prejuízos significativos ao Erário Público.

12. DO ACORDO DE NÍVEL DE SERVIÇO (ANS/SLA)

12.1. Para fins do que determina a Resolução TSE nº 23.234/2010, a empresa a ser contrata assumirá as seguintes condições de nível de serviço:

CONDIÇÃO	PRAZO/FORMA	CONDIÇÃO DE FALHA E ANS	MULTA
Disponibilizar Central de Atendimento no Brasil para abertura de chamado de Assistência Técnica, na modalidade 24/7.	- 24 horas por dia, 07 dias por semana.	Indisponibilidade da Central de Atendimento	(-) 0,1 % por hora de indisponibilidade sobre o valor do ITEM 1.– cumulada com demais penalidades.
Início da prestação do serviço de suporte após a abertura do chamado.	- Atendimento / encaminhamento de chamado de suporte técnico em até duas horas.	Atraso no início do atendimento / encaminhamento superior a 02 horas.	(-)0,1 % por ocorrência sobre o valor do ITEM 1.
Encerramento dos chamados técnicos	- atendimento de acordo com os prazos estabelecidos na Tabela 2 e Tabela 3	Atraso na conclusão do atendimento de acordo com os prazos estabelecidos	(-)0,1 % por ocorrência sobre o valor do ITEM 1.
Substituir equipamento defeituoso conforme chamado técnico.	- Substituir o equipamento defeituoso em até 5 (cinco) dias corridos após análise do chamado técnico cujos prazos estão estabelecidos na Tabela 2 e Tabela 3.	Atraso na substituição do equipamento	(-)0,5 % por dia de atraso sobre o valor do material a ser substituído, limitado a 10 (dez) dias corridos.

12.2. A multa será limitada a 10% do valor total de contratação.

12.2.1. A indisponibilidade da Solução resultante da ausência de prestação por parte da empresa contratada será considerada descumprimento parcial da contratação e corresponderá a aplicação da penalidade de multa sobre o valor total da contratação;

12.2.2. O Secretário da STI, a pedido da equipe técnica, poderá suspender os prazos do SLA/ANS se entender pertinente, desde que observe a possiblidade de mitigação dos riscos, ou que inexista prejuízos ao erário público, ou ao andamento normal dos trabalhos desenvolvidos nesta Corte por prazo não superior a 30 (trinta) dias para troca de equipamentos e 5 dias para os demais casos;

12.2.3. Quando a equipe técnica solicitar a suspensão dos serviços para prevenir a indisponibilidade da Solução, suspender-se-ão os prazos do ANS.

13. PENALIDADES (SANÇÕES)

13.1. Vide edital.

14. VIGÊNCIA DO CONTRATO

14.1. O contrato, resultante das aquisições, nos termos da resolução TSE 23.234/2010, terá vigência de 60 (sessenta) meses;

14.1.1. Durante a vigência do contrato, este Tribunal, a seu critério, obedecendo ao limite de 25% (vinte e cinco por cento) do valor total da contratação, poderá aditar o quantitativo de serviços e treinamentos, de modo a manter a solução atualizada e garantir os objetivos estratégicos justificados.;

14.1.2. Se considerado vantajoso, a critério do Tribunal Regional Eleitoral de Mato Grosso (pesquisas de mercado e comparações com outras contratações) e atender à estratégia desta Corte, o contrato poderá ser prorrogado;

14.1.3. No caso de aditamento ou prorrogação, o valor a ser considerado como o do contrato, será aquele das aquisições efetuadas, corrigido anualmente pelo IPCA até a data da solicitação do aditamento.

14.2. No momento da assinatura do contrato, a empresa licitante deverá comprovar que possui, pelo menos, um profissional, certificado pela Fabricante nas funcionalidades contratadas, com experiência mínima de dois anos na área de segurança de redes e /ou segurança da informação. A comprovação deverá ser encaminhada juntamente com o contrato após a assinatura.

15. DO PAGAMENTO

15.1. O pagamento será creditado em nome da Contratada, mediante ordem bancária em conta corrente por ela indicada ou por meio de ordem bancária para pagamento de faturas com código de barras, uma vez satisfeitas as condições estabelecidas neste instrumento;

15.2. No caso de processamento do pagamento através de depósito bancário, deverão ser fornecidos os seguintes dados: a) banco; número, nome e código; b) agência: número e código e c) número da conta corrente (completo) juntamente com a nota fiscal/fatura;

15.3. O pagamento será realizado mediante apresentação de Nota Fiscal/Fatura pela Contratada, para que seja lavrada certidão de seu recebimento ou atestada sua execução irregular de forma devidamente circunstanciada, o que implicará, neste caso, a interrupção do prazo para pagamento;

15.4. A data de vencimento da fatura nunca poderá ser inferior a 30 (trinta) dias da data de seu efetivo encaminhamento ao Tribunal;

15.5. Na nota fiscal ou documentos anexos, deverão ser descriminados os serviços;

15.6. O pagamento será efetivado no prazo máximo de 30 (trinta) dias;

15.6.1. No caso de o setor responsável pelo pagamento verificar a ocorrência de irregularidade fiscal ou trabalhista por parte da Contratada, deverá comunicar à Administração para a adoção e medidas administrativas pertinentes.

15.7. Será efetuada a retenção de tributos por ocasião do pagamento das Notas Fiscais/Faturas emitidas por pessoas jurídicas, pela prestação de serviços em geral, conforme normas que regulamentam o artigo 64, da Lei 9.430 de 27/12/96, se for o caso, bem como aquelas afetas aos serviços de tecnologia de informação e comunicação;

15.8. As empresas inscritas no SIMPLES NACIONAL não estão sujeitas à aplicação da tabela de retenção na fonte, desde que apresentem a este Tribunal, junto à Nota Fiscal/Fatura, Declaração em conformidade com as normas que regulamentam o artigo 64 da Lei 9.430/96;

15.9. O Tribunal poderá deduzir do montante a pagar os valores correspondentes a multas, glosas ou indenizações devidas pela Contratada;

15.10. O processamento da ordem bancária com observância dos dados fornecidos pela Contratada constitui prova de quitação da obrigação para todos os efeitos legais, ficando a contratada responsável por quaisquer contratempos decorrentes da apresentação inexata dos dados fornecidos;

15.11. Se ocorrerem eventuais atrasos de pagamento provocados exclusivamente por culpa da Administração, o valor devido deverá ser acrescido de atualização financeira, e sua apuração se fará desde a data de seu vencimento até a data do efetivo pagamento. Para tanto, os juros de mora serão calculados à taxa de 0,5% (meio por cento) ao mês (seis por cento ao ano), mediante aplicação das seguintes fórmulas:

I= (TX/100)/365

EM = I x N x VP

Onde:

I = índice de atualização financeira;

TX = Percentual da taxa de juros de mora anual;

EM = Encargos moratórios;

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

pagamento; e

VP = Valor da parcela em atraso.

16. DA PROPOSTA E DOCUMENTOS

16.1. A licitante vencedora deverá apresentar em sua proposta:

16.1.1. Documentos contendo as especificações técnicas detalhadas contendo os códigos dos serviços da Fabricante a serem cobertos pelo contrato de suporte e sua relação com todos os equipamentos e softwares objetos desta licitação. Na eventualidade de mudança dos códigos de serviço durante o processo licitatório, a proposta deverá constar a correlação entre os códigos antigos e os novos;

16.1.2. E-mail para contato para tratamento dos assuntos relativos à contratação – sendo este meio de comunicação considerado oficial para fins de recebimento e envio de informações, pedidos, documentos, comunicados e notificações;

16.1.3. E-mail e/ou telefone e/ou site da central de serviços para abertura de chamado técnico, bem como os procedimentos e dados que serão necessários para abertura e registro de chamados técnicos para a prestação da assistência técnica e garantia;

16.1.4. Um atestado de capacidade técnica onde a Licitante figure como fornecedora de serviço de suporte de Solução de Segurança, baseada na tecnologia da Fabricante, com as tecnologias de WAF e balanceamento de carga.

16.1.5. A ementa das capacitações;

16.2. DA PROPOSTA

16.3. As licitantes deverão ofertar propostas de preços por lote único, da seguinte forma:

LOTE ÚNICO:

ITEM	PRODUTOS	QTD	VL. UNIT.	VALOR TOTAL
01	*Appliance* Web Application Firewall e balanceador de carga	02	R$	R$
02	Serviço de instalação e configuração da solução	01	R$	R$
03	Capacitação	04	R$	R$

TOTAL: R$ _____

16.4. O Tribunal, durante toda a vigência do contrato e, principalmente, até a data da entrega, poderá solicitar documentos que comprovem a capacidade técnica e financeira da empresa contratada e outros documentos comprobatórios que julgue importante para garantir a segurança da informação e a continuidade dos serviços, tendo em vista, a priorização dos Objetivos Estratégicos que norteiam esta contratação.

17. DOS RECURSOS ORÇAMENTÁRIOS

17.1. Os recursos para a execução do objeto deste Termo de Referência serão aqueles consignados no Orçamento da Justiça Eleitoral para o ano de 2021, 2022 e, também, obtidos via créditos suplementares.

18. ESTIMATIVA DE CUSTO

18.1. A estimativa formal de custo é aquela apresentada na Tabela 2.

18.2. Os valores constantes na estimativa disponibilizada serão atualizados com base naqueles aferidos pelo setor responsável por coletas de preços neste Tribunal.

ITEM	PRODUTOS	QTD	VL. UNIT. (R$)	VALOR TOTAL (R$)
01	*Appliance* Web Application Firewall e balanceador de carga	02	735.698,76	1.471.397,52
02	Serviço de instalação e configuração da solução	01	86.046,64	86.046,64
03	Capacitação	04	R$31.277,00	125.108,00
	Total		853.022,40	1.682.552,16

Tabela 2. Estimativa de custos.

18.3. LOTE ÚNICO: As estimativas estabelecidas foram baseadas nos contratos TSE nº. 43/2019 e Ministério da Educação nº. 28/2019 incluindo a correção da cotação do dólar e o ajuste para a quantidade de *features* a serem contratadas – apenas para estimativa inicial.

ANEXO I – ESPECIFICAÇÃO TÉCNICA

1. DA ESPECIFICAÇÃO TÉCNICA DOS APPLIANCES E FUNCIONALIDADES (ITEM 1)

1.1. DA CARACTERÍSTICA DE HARDWARE E DESEMPENHO INDIVIDUAL DOS APPLIANCES.

1.1.1.O equipamento deverá ser novo, de primeiro uso e acondicionado adequadamente em caixa lacrada de fábrica, de forma a propiciar completa segurança durante o transporte;

1.1.2.O equipamento do tipo *appliance*, deve possuir altura de, no máximo, 2U, para ser instalado em rack de 19” e ser fornecido com o kit de instalação;

1.1.3.O equipamento deve possuir capacidade de processamento e memória suficiente para operar com todas as funcionalidades contratadas simultaneamente e no volume máximo de tráfego descrito neste Termo de Referência;

1.1.4.O equipamento deve possuir fontes redundantes, do tipo hot *swappable*, 100-240V com seleção automática de tensão;

1.1.5.O equipamento deve possuir, no mínimo, de 01 (uma) porta console para configuração através de CLI (*Command Line Interface*);

1.1.6.O equipamento deve possuir, no mínimo, 4 (quatro) *interfaces* Gigabit Ethernet (1000BASE-T) e 2 (duas) *interfaces* 10 (dez) Gigabit Ethernet incluindo os *tranceivers* SFP+ ;

a) Todas as *interfaces* fornecidas no *appliance* devem estar licenciadas e habilitadas para uso imediato;

b) Deve ser fornecido com 4 (quatro) *transceivers* SFP+ SR(10 Gbps);

1.1.7.Possuir painel de LCD frontal com indicação de status do equipamento e capacidade para reiniciar/desligar o sistema;

1.1.8.Possuir capacidade para tratar 300.000 (trezentas mil) requisições por segundo em camada 7 (sete);

1.1.9.Possuir capacidade para tratar 100.000 (cem mil) conexões por segundo em camada 4 (quatro);

1.1.10.Possuir capacidade para sustentar, no mínimo, 10.000.000 (dez milhões) de conexões simultâneas em camada 4 (quatro);

1.1.11.Possuir capacidade mínima de *throughput,* em camada 4 (quatro), de 10 (dez) Gbps (Gigabits por Segundo);

1.1.12.Possuir capacidade mínima de *throughput,* em camada 7 (sete), de 5 (cinco) Gbps.

1.1.13.Ser capaz de tratar, pelo menos, 2.100 (duas mil e cem) transações SSL/TLS por segundo (TPS) considerando *Elliptic Curve Digital Signature Algorithm* (ECDSA) P-256;

1.1.14.Ser capaz de tratar, pelo menos, 2.500 (duas mil e quinhentas) transações SSL/TLS por segundo (TPS) considerando *Rivest-Shamir-Adleman* (RSA) com chaves de 2048 bits;

1.1.15.Possuir capacidade de criptografar com *throughput* mínimo de 5 (cinco) Gbps;

1.1.16.Todas as funcionalidades deverão ser fornecidas pelo mesmo fabricante, de maneira integrada, incluindo o sistema operacional.

1.2. DAS CARACTERÍSTICAS GERAIS

1.2.1.A solução deve permitir a instalação em ambientes de alta disponibilidade das seguintes formas:

a) Ativo/Standby, com equipamento da mesma marca e modelo;

b) Ativo/ativo, com equipamento da mesma marca e modelo, mantendo o status das conexões. Entende-se como ativo/ativo a utilização de dois endereços virtuais, onde cada endereço está ativo em um elemento e standby no outro ou a capacidade do mesmo endereço virtual ser respondido de forma controlada pelos dois elementos simultaneamente.

1.2.2.A solução deve possuir gerência centralizada ou sincronização de gerências, caso sejam individuais, a partir da configuração do ambiente de alta disponibilidade e tolerância a falhas;

a) Todas as licenças de gerenciamento necessárias para o correto funcionamento da solução, de acordo com os requisitos estipulados neste Termo de Referência, devem ser fornecidas em conjunto com a solução.

1.2.3.A solução deve implementar, quando em alta disponibilidade, sincronismo de sessão entre os elementos, onde a falha do equipamento principal não deverá causar a interrupção das sessões balanceadas;

1.2.4.A solução deve fornecer todos os recursos de redundância sem despesas adicionais com licenças;

1.2.5.A solução deve permitir escalabilidade, podendo escalar horizontalmente, na forma de cluster, adicionando novos *appliances,* inclusive, de modelos diferentes;

1.2.6.A solução deve fornecer recurso de agregação de portas baseado no protocolo LACP (*Link Aggregation Control Protocol*), suportando os modos passivo e ativo;

a) A solução deve fornecer recurso para suportar, no mínimo, 4 (quatro) portas em um mesmo conjunto agregado;

1.2.7.A solução deve suportar os protocolos *Spanning-Tree*(802.1D), *Fast Spanning-Tree* (802.1w, 802.1t) e *Multi Spanning-Tree* (802.1s);

1.2.8.A solução deve suportar o protocolo 802.1q;

1.2.9.A solução deve suportar o protocolo SNTP (*Simple Network Time Protocol*) ou NTP (*Network Time Protocol*);

1.2.10. A solução deve suportar IPv6;

1.2.11.A solução deve suportar LLDP (*Link Layer Discovery Protocol*);

1.2.12.A solução deve suportar múltiplas tabelas de rotas independentes;

1.2.13.A solução deve possuir capacidade para gerenciar os recursos disponíveis de acordo com as funções habilitadas;

1.2.14.A solução deve permitir múltiplos domínios de roteamento em IPv4 e IPv6;

1.2.15.A solução deve permitir a configuração de endereçamento IP estático ou dinâmico (DHCP/BOOTP) para o gerenciamento;

1.2.16.A solução deve permitir a administração remota através de SSH;

1.2.17.A solução deve permitir manter internamente múltiplos arquivos de configurações do sistema;

1.2.18.A solução deve suportar transferência de arquivos de configuração e Sistema Operacional utilizando SCP ou HTTPS;

1.2.19.A solução deve permitir acesso por *Interface* de linha de comando (CLI – *Command Line Interface*), possibilitando a configuração dos equipamentos com acesso via porta de console e SSH com, no mínimo, as seguintes facilidades:

a) Função de auto completar de comandos na CLI;

b) Ajuda contextual dos comandos na CLI;

c) Comando para visualizar o tráfego de utilização das interfaces em bits/segundo (bps) e pacotes/segundo (pps);

d) Reinicialização do equipamento por comando na CLI;

e) Ferramentas para identificação de problemas (*debugging*) através da CLI;

f) Criação de, no mínimo, três níveis de usuários na GUI – administrador, usuário com permissões reduzidas e usuário somente leitura;

1.2.20.A solução deve permitir a autenticação dos usuários de gerência em bases remotas e suportar no mínimo RADIUS e LDAP;

1.2.21.A solução deve possuir interface gráfica web com acesso seguro utilizando HTTPS;

1.2.22.A solução deve permitir a atualização do sistema operacional e/ou a instalação de *patches* ou *Hotfixes* através da interface Gráfica sem o uso da linha de comando;

1.2.23.A solução deve suportar a restauração (*rollback*) de configuração e sistema operacional;

1.2.24.A solução deve fornecer geração de mensagens de Syslog para eventos relevantes ao sistema;

a) A solução deve possibilitar a configuração de múltiplos servidores Syslog para os quais o equipamento irá enviar as mensagens de Syslog;

b) A solução deve armazenar as mensagens de Syslog em dispositivo interno ao equipamento.

1.2.25.A solução deve permitir a reinicialização dos equipamentos a partir da interface gráfica;

1.2.26.A solução deve possuir recurso de gerência via SNMP (*Simple Network Management Protocol*) e implementar SNMPv1, SNMPv2c e SNMPV3:

a) A Solução deve permitir a criação de MIBs customizadas;

b) A solução deve Implementar envio de notificações (traps) via SNMP;

1.2.27.A solução deve suportar sFlow.

1.3. DAS CARACTERÍSTICAS DE BALANCEAMENTO DE CARGA, OTIMIZAÇÃO E DISPONIBILIDADE.

1.3.1.A solução deve suportar todas as aplicaçes comuns de um Switch *Layer* 7, como:

a) *Server Load-Balancing*;

b) *Firewall Load-Balancing*;

c) *Proxy Load-Balancing*.

1.3.2.A solução deve suportar balanceamento apenas em direço ao servidor, onde a resposta do servidor real é enviada diretamente ao cliente;

1.3.3.A solução deve permitir o encapsulamento, em camada 3, do trafego entre o balanceador de carga e o servidor, considerando trafego IPv4 e IPv6, quando o balanceamento é realizado apenas em direção ao servidor;

1.3.4.A solução deve permitir a clonagem de *pools*, de forma que a solução envie uma cópia do trafego para um *pool* adicional, para fins de análise do tráfego de dados;

1.3.5.A solução deve possuir recursos para balancear servidores com qualquer *hardware*, sistema operacional e tipo de aplicação;

1.3.6.A solução o deve possuir recurso de ativação de grupo prioritário, permitindo especificar a quantidade mínima de servidores que devem estar disponíveis em cada grupo e a prioridade dos grupos;

a) Caso o número de servidores disponíveis se torne inferior ao estipulado, a solução deve, automaticamente, distribuir o tráfego para o próximo grupo com maior prioridade, não afetando o serviço.

b) Caso o número de servidores disponíveis volte ao valor mínimo configurado, a solução deve, automaticamente, retirar o grupo com menor prioridade do balanceamento, voltando ao estado original.

1.3.7. A solução deve possuir capacidade de estabelecer conexões TCP prévias com o servidor e inserir as requisições HTTP geradas pelos clientes nessas conexões, reduzindo, assim, a necessidade de estabelecimento de conexões nos servidores, aumentando a performance do serviç;

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

a) Round Robin;

b) *Least Connections*;

c) *Weighted Percentage* (por peso);

d) Servidor ou equipamento com resposta mais rápida baseado no tráfego real;

e) *Weighted Percentage* dinâmico (baseado no número de conexões)

f) Dinâmico, baseado em parâmetros de um determinado servidor ou equipamento, coletados via SNMP.

1.3.9.A solução deve permitir aplicar criptografia de *cookies*;

1.3.10.A solução deve possuir recursos para balancear as sessões novas, preservando as sessões existentes no mesmo servidor, implementando persistêcia de sessão dos seguintes tipos:

a) Por *cookie*: inserção de um novo cookie na sessão;

b) Por *cookie*: utilização do valor do cookie da aplicação, sem adição de cookie;

c) Por endereço IP destino;

d) Por endereço IP origem;

e) Por sessão SSL;

f) Através da análise da URL acessada.;

g) Através da análise de qualquer parâmetro no *header* HTTP;

h) Através da análise de sessões do MSRDP (MS *Terminal Desktop Protocol*);

i) Através da análise do *SIP Call ID* ou *Source* IP;

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

1.3.11.A solução deve utilizar CARP (*Cache Array Routing Protocol)* no algoritmo de *HASH*;

1.3.12.A solução deve suportar, no mínimo, o monitoramento dos servidores reais através de protocolos de camada 3 e 4.

1.3.13.A solução deve disponibilizar monitores predefinidos para, no mínimo, os seguintes protocolos e servidores: ICMP, HTTP, HTTPS, Diameter, FTP, SASP, SMB, RADIUS, MSSQL, NNTP, ORACLE, RPC, LDAP, IMAP, SMTP, POP3, SIP, Real Server, SOAP, SNMP e WMI;

1.3.14.A solução deve possuir funcionalidades para:

a) Balancear carga de servidores SIP para VoIP (equipamento SIP PROXY);

b) Limitar o número de sessões estabelecidas com cada servidor real;

c) Limitar o número de sessões estabelecidas com cada servidor virtual;

d) Limitar o número de sessões estabelecidas com cada grupo de servidores;

e) Limitar o número de sessões estabelecidas com cada servidor físico;

f) Realizar *Network Address Translation* (NAT);

g) Realizar proteção contra *Denial of Service* (DoS), incluindo *Syn Flood;*

h) Realizar Limpeza de cabeçalho HTTP;

1.3.15.A solução deve permitir o controle da resposta ICMP por servidor virtual;

1.3.16.A solução deve possuir recursos para que a configuração seja baseada em perfis.

1.3.17.A solução deve possuir capacidade de geração e gestão de perfis hierarquizados, permitindo maior facilidade na administração de políticas similares;

1.3.18.A solução deve possuir permitir a criação de Virtual Servers com endereços IPv4 e os servidores reais com endereços IPv6;

1.3.19.A solução deve possuir recursos para executar compressão de conteúdo HTTP, reduzindo a quantidade de informações enviadas ao cliente, permitindo a definição de qual algoritmo de compressão deverá ser habilitado, incluindo:

a) gzip1 a gzip9;

b) Deflate.

1.3.20.A solução deve possuir capacidade para definir compressão especificamente para certos tipos de objetos;

1.3.21.A solução deve possuir recursos acelerar SSL, onde os certificados digitais são instalados no equipamento e as requisições HTTP, POP3S, IMAPS e SMTPS são enviadas aos servidores sem criptografia.

a) A solução deve garantir que na aceleração de SSL seja realizada com aceleração em hardware, tanto para troca de chaves quanto para criptografia dos dados.

1.3.22.A solução deve possuir capacidade de importação dos certificados e chaves criptográficas de serviços e da cadeia de certificadoras, podendo, assim, operar em modo "*man in the middle*.

a) Havendo falha na leitura da conexão SSL, esta deverá, se configurado, prosseguir em regime de *passthrough*.

1.3.23.A solução deve possuir a funcionalidade de espelhamento de conexões SSL, HTTP e UDP .

1.3.24.A solução deve possuir a capacidade de redirecionar o SSL *offload* (troca de chaves) de determinado serviço para outro *appliance* físico que tenha mais capacidade para tratamento SSL;

1.3.25.A solução deve permitir a configuração para criptografar novamente em SSL a requisição ao enviar para o servidor, permitindo as demais otimizaçes em ambiente 100% (cem por cento) criptografado;

1.3.26.A solução deve disponibilizar todas as funcionalidades de inspeço, proteço e aceleraço de tráfego criptografado, através de SSL/TLS, especificados neste Termo de Referência, independentemente se a autenticação está sendo realizada na extremidade do cliente ou do servidor ou de ambos simultaneamente;

1.3.27.A solução deve realizar inspeço, proteço, *offload* e aceleraço de tráfego criptografado através de SSL/TLS, devendo ser capaz de:

a) 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;

b) Encaminhar ao servidor real via, cabeçalho HTTP, campos específicos do certificado digital utilizado pelo cliente para se autenticar perante o servidor durante o processo de estabelecimento do túnel SSL/TLS.

1.3.28.A solução deve permitir aplicar criptografia de *cookies* para a proteço dos mesmos;

1.3.29.A solução deve permitir a configuração, no mínimo, dos seguintes recursos relacionados ao uso de criptografia com o objetivo de otimizar e minimizar o impacto na *performance* das aplicaçes:

a) SSL *Session Cache Timeout*;

b) *Session Ticket*;

c) OCSP (*Online Certificate Status Protocol*) *Stapling*;

d) Dynamic Record Sizing;

e) ALPN (*Application Layer Protocol Negotiation*);

f) Perfect Forward Secrecy.

1.3.30.A solução deve suportar a utilizaço de memória DRAM (*Dynamic Random Access Memory*) como cache de objetos HTTP, permitindo selecionar quais tipos de objetos serão armazenados, permitindo, inclusive, configurar a quantidade de memória reservada para cache.

1.3.31.A solução deve suportar a otimização de parâmetros das conexões TCP.

1.3.32.A solução deve suportar ICAP (Internet *Content Adaptation Protocol*).

1.3.33.A solução deve ser capaz de realizar DHCP relay;

1.3.34.A solução deve possuir relatórios em tempo real das aplicações es, com gráficos, com pelos menos os seguintes dados:

a) Tempo de resposta da aplicação;

b) Latência;

c) Conexões estabelecidas por servidor ou conjunto de servidores;

d) Por URL (*Uniform Resource Locator*);

1.3.35.A solução deve permitir a geração de gráficos na ferramenta de relatórios com, no mínimo, os seguintes filtros:

a) Servidores virtuais;

b) Servidores balanceados;

c) URLs.

d) Países de origem, baseados em geolocalização (GEOIP);

e) Dispositivos de origem do cliente (User Agent);

1.3.36.A solução deve possuir *framework* unificado para configuração da aplicação.

1.3.37.A solução deve suportar a comunicação entre os balanceadores por de túneis IPSec.

1.3.38.A Solução deve ter a capacidade de permitir a criação de MIBs (*Management Information Base*) customizadas;

1.3.39.A solução de permitir que os domínios de roteamento utilizem OSPF (*Open Shortest Path First*) em IPv4 e Ipv6.

1.3.40.A solução deve suportar ECMP (*Equal Cost Multipath*);

1.3.41.A solução deve realizar BFD (*Bidirectional Forward Detection*);

1.3.42.A solução deve ter suporte a *Transport Layer Security* (TLS) Server *Name Indication* (SNI);

1.3.43.A solução deve possuir monitor HTTP/HTTPS com autenticação NTLM embutida, que permita verificar se o HTTP/HTTPS está operando assim como a plataforma de autenticação;

1.3.44.A solução deve ter suporte a TLS 1.2, SHA 2 *Cipher* e SHA256 *Hash*;

1.3.45.A solução deve ter suporte a criptografia *Perfect Forward Secrecy* não apenas para troca de chaves RSA.

1.3.46.A solução deve ser capaz de colocar em fila as requisiçes TCP que excedam a capacidade de conexões do grupo de servidores ou de um servidor, não descartando, assim, as conexões que excedam o número de conexões do servidor e de um grupo deles;

a) Deve ser possível configurar o tamanho máximo da fila;

b) Deve ser possível configurar o tempo máximo de permanência na fila;

1.3.47.A solução deve realizar controle de banda estático para grupos de aplicaçes e rede;

1.3.48.A solução deve realizar controle de banda dinâmico por aplicação e usuário;

1.3.49.A solução deve realizar controle de banda baseado em domínio de roteamento;

1.3.50.A solução deve permitir tráfego por parâmetros de QoS (*Quality of Service*) ou *rate-shaping,*baseada na camada de aplicaço;

1.3.51.A solução deve permitir a priorizaço de tráfego de entrada por aplicaçes;

1.3.52.A solução deve permitir a criação de túneis IP por domínio de roteamento utilizando GRE, IPIP e PPP;

1.3.53.A solução deve permitir a criaço de tuneis IP transparente utilizando GRE e IPIP;

1.3.54.A solução deve possuir suporte ao protocolo SPDY e HTTP 2.0;

1.3.55.O equipamento deverá permitir a sincronização das configurações de forma automática e manualmente;

1.3.56.A solução deve permitir que regras customizadas em linguagem aberta possam ser utilizadas para customizar a distribuiço dinâmica de tráfego;

1.3.57.A solução deve permitir a manipulação do tráfego de entrada e saída, inclusive com a importação de pacotes de códigos, viabilizando, assim, a alteração de parâmetros no cabeçalho e no corpo das mensagens:

1.3.58.A solução deve permitir a criaço de políticas através de interface web para manipulaço de tráfego para, pelo menos, os operadores GEOIP, http-basic-auth, http-cookie, http-header, http-host, http-method, http-referer, http-set-cookie, http-status, http-uri e http-version, devendo ser possível executar as seguintes ações;

a) Bloqueio de tráfego;

b) Reescrita e manipulação de URL;

c) Registro de tráfego (log);

d) Adição de informação no cabeçalho HTTP;

e) Redirecionamento do tráfego para um membro específico;

f) Selecionar uma política específica para Aplicação Web;

1.3.59.A solução deve ser capaz de fazer log de todas as sessões, onde os registros deverão conter, no mínimo, as seguintes informações:

a) Endereços IP de origem e destino;

b) Portas de origem e destino;

c) Protocolo de camada 4 (TCP ou UDP);

d) Data e hora;

e) URL;

1.3.60.A solução deve possuir políticas de uso de senhas administrativas, de forma nativa ou integrado a uma base *Active Directory*, tais como: nível de complexidade, período de validade e travamento de conta devido a erros múltiplos de *login*;

1.3.61.A solução deve suportar controle de versão da política de configuração de forma a permitir a restauração de políticas aplicadas.

1.3.62.A soluçãodeve ser capaz de analisar a *performance* de aplicaçes web.

1.3.63.A solução deve prover métricas de aplicaçes como: transaçes por segundo; tempo de latêcia do cliente e servidor; *throughput* de requisições e respostas;

1.3.64.A solução deve gerar informações para análises históricas e apoio nos processos de manutenções preventivas, de *troubleshooting*, de planejamento de capacidade e de análise da experiência dos usuários finais no acesso das aplicações;

a) As informações coletadas deverão permitir a análise dos dados por aplicações, por URL's, por clientes e por servidores, permitindo assim a identificação mais precisa dos eventuais ofensores do tráfego suportado pela solução;

b) A geração de informações históricas deverá permitir o detalhamento do tempo de resposta total de carregamento de uma URL e/ou Página, bem como permitir a correlação de métricas de uso de rede com o comportamento das aplicações.

1.3.65.A solução deve gerar informações estatísticas de acesso identificando, para cada aplicação, os métodos de acesso HTTP (GET e Post), o tipo de sistema operacional utilizado pelos clientes, e os browsers utilizados.

1.4. DAS CARACTERÍSTICAS DA SOLUÇÃO DE WEB APPLICATION FIREWALL (WAF)

1.4.1.A solução deve proteger a infraestrutura web de ataques contra a camada de aplicação (Camada 7);

1.4.2.A solução deve possuir tecnologia para mitigação de ataques DoS (*Deniel of Service*), baseados na camada 7, incluindo análise comportamental do tráfego de dados e *stress* do servidor de aplicações;

a) Ao detectar uma condição de DoS, regras de proteção devem ser automaticamente criadas e implementadas em tempo real para proteção da aplicação;

b) Os valores limiares de DoS devem ser auto ajustáveis e adaptativos de acordo com as mudanças;

c) Deve permitir apenas registrar o ataque, sem tomar nenhuma ação de bloqueio;

1.4.3.A solução deve possuir as seguintes formas de detecção de ataques DoS na camada de aplicação:

a) Número de requisições por segundo enviados a uma URL específica;

b) Número de requisições por segundo enviados de um IP específico;

c) Detecção através de código executado no cliente com o objetivo de detectar interação humana ou comportamento de robôs (*bots*);

d) Número máximo de transações por segundo (TPS) de um determinado IP;

e) Aumento de um determinado percentual do número de transações por segundo (TPS).

1.4.4.A solução deve prevenir ataques de *Credential Stuffing*;

1.4.5.A solução deve possuir a capacidade de capturar tráfego no formato *TCP Dump* relativos aos ataques de DoS L7, *Web Scraping* e força bruta;

1.4.6.A solução deve suportar o uso de firewall *full state* junto com o firewall camada 7, nos mesmos *applicances*;

1.4.7.A solução deve permitir a utilização de um modelo positivo de segurança para proteger contra ataques conhecidos aos protocolos HTTP e HTTPS e, também, às aplicações web acessíveis através destes, incluindo aqueles que constam no OWASP TOP-10;

1.4.8.A solução deve possuir política de segurança de aplicações web predefinidas na solução;

1.4.9.A solução deve permitir a criação de políticas diferenciadas por aplicação e por URL, onde cada aplicação e URL poderão ter políticas totalmente diferentes;

1.4.10.A solução deve permitir configurar de forma granular, por aplicação protegida, restrições de métodos HTTP permitidos, tipos ou versões de protocolos, tipos de caracteres e versões utilizadas de cookies;

1.4.11.A solução deve permitir a inspeção de *upload* de arquivos para os servidores de aplicação;

a) A inspeção pode ser feita via integração ICAP, permitindo a integração com diferentes softwares de Antivírus;

1.4.12.A solução deve permitir a integração com *firewall* de banco de dados e análise de logs de outros fabricantes;

1.4.13.A solução deve permitir que regras customizadas, em linguagem aberta, possam ser utilizadas para customizar e aumentar a proteção contra ataques recentes;

1.4.14.A solução deve possuir tecnologia de detecção de anomalias baseado em rastreamento de identificação de dispositivos, permitindo a detecção de ataques DoS, de força bruta e de sequestro de sessão.

a) Deve ser possível filtrar relatórios por identificação de dispositivos;

1.4.15.A solução deve permitir incluir em B*lacklist* os endereços IPs que repetidamente falharem a desafios no navegador:

a) Ao entrar em *Blacklist*, a solução deverá bloquear automaticamente os pacotes enviados pelo endereço bloqueado por um período de tempo;

1.4.16.A solução deve prover suporte e proteger o tráfego de dados encapsulado no protocolo WebSocket;

1.4.17.A solução deve possuir funcionalidade de proteção positiva e segura contra ataques, incluindo pelo menos:

a) Acesso por Força Bruta, incluindo no navegador;

b) Ameaças Web AJAX/JSON;

c) DoS e DDoS de camada 7;

d) *Buffer Overflow*;

e) *Cross Site Request Forgery* (CSRF);

f) *Cross-Site Scripting* (XSS);

g) SQL Injection;

h) *Parameter tampering*;

i) Cookie poisoning;

j) HTTP *Request Smuggling*;

k) Manipulação de campos escondidos e cookies;

l) Roubo de sessão através de manipulação de cookies;

m) Sequestro de sessão;

n) XML bombs/DoS.

1.4.18.A solução deve suportar o uso de páginas de login AJAX/JSON, com configuração manual e descoberta automática;

1.4.19.A solução deve possuir proteção baseada em assinaturas para prover proteção contra ataques conhecidos;

a) Deve permitir desabilitar algumas assinaturas específicas, em determinados parâmetros, como uma exceção a regra geral;

b) A atualizações de assinaturas deverão passar por um período configurável de testes, ondes nenhuma requisição que viole a assinatura será bloqueada, apenas informada no relatório. Este processo deve ser automatizado, não sendo necessário criar regras específicas a cada atualização de assinatura;

c) As assinaturas devem ser atualizadas periodicamente pela base do fabricante, devendo as atualizações ocorrerem durante o período contratado de subscrição não gerando custos adicionais para a CONTRANTE na aquisição de novas licenças ou subscrições;

1.4.20.A solução deve ser capaz de identificar e bloquear ataques através de regras de verificação personalizadas;

1.4.21.A solução deve permitir a customização da resposta de bloqueio;

1.4.22.A solução deve permitir a liberação temporária, ou definitiva, (*Whitelist*) de endereços IP bloqueados por terem originados ataques detectados pela solução;

1.4.23.A solução deve permitir limitar o número de conexões e requisições por IP de origem para cada endereço IP Virtual;

a) A solução deve permitir adicionar, automaticamente e manualmente, em uma lista de bloqueio, os endereços IP de origem que ultrapassarem o limite estabelecido, por um período determinado através de configuração;

1.4.24.A solução deve permitir criar lista de exceção (whitelist) por endereço IP específico ou faixa de sub-rede;

1.4.25.A solução deve permitir o uso do parâmetro HTTP *X-Forwarded-For* como parte da política de controle;

1.4.26.A solução deve implantar, no mínimo, as seguintes funcionalidades:

a) Checagem de URL;

b) Checagem de métodos HTTP utilizados (GET, POST, HEAD, OPTIONS, PUT, TRACE, DELETE, CONNECT);

c) *Cookie Encryption*;

d) Checagem de consistência de formulários;

e) Checagem do cabeçalho "*user-agent*" para identificar clientes inválidos.

1.4.27. A solução deve implementar funcionalidades para proteção contra exposição de informações do ambiente e servidores internos (*Cloaking*), incluindo pelo menos:

a) Informações que identifique o sistema operacional e o servidor web através de "impressão digital" dos sistemas;

b) Esconder qualquer mensagem de erro HTTP dos usuários;

c) Remover as mensagens de erro às páginas que serão enviadas aos usuários.

1.4.28 A solução deve permitir a utilização de uma página HTML informativa e personalizável como HTTP Response aos bloqueios;

1.4.29.A solução deve verificar o endereço de origem do pacote IP no cabeçalho IP e no parâmetro *X-forwarded-for* (XFF);

1.4.30.A solução deve suportar a criação de políticas por geolocalização, permitindo que o tráfego de determinado(s) país/países seja(m) bloqueado(s);

1.4.31.A solução deve possuir mecanismo de aprendizado automático capaz de identificar todos os conteúdos das aplicações, incluindo URLs, parâmetros das URLs, campos de formulários, o que se espera

de cada campo (tipo de dado, tamanho de caracteres), *cookies*, arquivos XML e elementos XML;

1.4.32.A solução deve possuir funcionalidade de criação automática de políticas, onde a política de segurança é criada e atualizada automaticamente baseando-se no tráfego real destinado à aplicação;

a) O perfil aprendido de forma automatizada pode ser ajustado, editado ou bloqueado.

1.4.33.A solução deve permitir o bloqueio de ataques de força bruta de usuário/senha em páginas de acesso (login). Este bloqueio deve limitar o número máximo de tentativas e o tempo do bloqueio deverá ser configurável;

1.4.34.A solução deve permitir o bloqueio de determinados endereços IPs que ultrapassarem um número máximo de violações por minuto.

a) O período de bloqueio deverá ser configurável e durante este período todas as requisições do cliente serão bloqueadas automaticamente.

1.4.35.A solução deve permitir o bloqueio de robôs (bots) que acessam a aplicação através de detecção automática, não dependendo de cadastros manuais.

a) Robôs conhecidos do mercado, como Google e Microsoft Bing deverão ser liberados por padrão;

b) Deve permitir o cadastro de robôs que podem acessar a aplicação;

1.4.36. A solução deve criptografar dados e credenciais na camada de aplicação, sem ter a necessidade de atualizar a aplicação;

1.4.37.A solução deve implementar proteção ao JSON (JavaScript Object Notation);

1.4.38.A solução deve possuir firewall XML integrado com suporte a filtro e validação de funções XML específicas da aplicação;

1.4.39.A solução deve Implementar a segurança de *Web Services*, através dos seguintes métodos:

a) Criptografar/Decriptografar partes das mensagens SOAP;

b) Assinar digitalmente partes das mensagens SOAP;

c) Verificação de partes das mensagens SOAP.

1.4.40.A solução deve proteger o protocolo FTP com pelo menos os seguintes métodos:

a) Determinar os comandos FTP permitidos;

b) *Requests* FTP anônimos;

c) Checar conformidade com o protocolo FTP;

d) Proteger contra ataques de força bruta nos *logins*;

1.4.41.A solução deve proteger o protocolo SMTP com pelo menos os seguintes métodos e características:

a) A comunicação deve ser aderente a RFC 2821;

b) Limitar o número de mensagens;

c) Validar registro SPF do DNS;

d) Determinar quais métodos SMTP podem ser utilizados.

1.4.42.A solução deve armazenar os registros (logs) localmente e permitir exportar para Syslog server;

1.4.43.A solução deve proteger contra atraques CSRF (*Cross-Site Request Forgery*), podendo ser possível especificar quais URLs serão examinadas;

1.4.44.A solução deve possuir controle de fluxo por aplicação, permitindo definir o fluxo de acesso de uma URL para outra da mesma aplicação.

a) 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.

1.4.45.A solução deve fornecer relatórios consolidados de ataques, permitindo o agendamento para entrega via e-mail, com, pelo menos, os seguintes dados:

a) Resumo geral com as políticas ativas;

b) Anomalias e estatísticas de tráfego;

c) Ataques de DoS, força bruta e robôs;

d) Violações, URL, endereços IP, países e severidade.

1.4.46.A solução deve fornecer gráficos de alertas, no mínimo, por:

a) Política de segurança;

b) Tipos de ataques;

c) Violações;

d) URL;

e) Endereços IP;

f) Países;

g) Severidade;

h) Código de resposta;

i) Métodos;

j) Protocolos;

k) Vírus;

l) Usuário;

m) Sessão.

1.4.47.A solução deve possuir relatório em tempo real sobre ataques de DoS L7, atualizado automaticamente;

a) Os logs devem indicar o momento de início e fim de um ataque de DoS L7.

1.4.48.A solução deve possuir lista dinâmica de endereços IP globais com atividades maliciosas, possuindo, no mínimo, as seguintes categorias de endereços:

a) *Windows Exploits*;

b) *Web Attacks*;

c) *Botnets*;

d) *Scanners*;

e) *Denial of Service*;

f) *Reputation*;

g) *Phishing Prox;*

h) Anonymous Proxy.

1.4.49.A solução deve possuir níveis de violação de uma requisição, permitindo classifica-las;

1.5. DA GARANTIA, SERVIÇO DE SUBSCRIÇÃO E SUPORTE

1.5.1.Todos os equipamentos e softwares envolvidos na solução deverão ser fornecidos com garantia do fabricante, serviço de suporte e subscrição para atualização diretamente com a fabricante por período de 60 (sessenta) meses;

1.5.2.A garantia dos produtos deverá contemplar e prestar, no mínimo, os seguintes serviços:

a) Atualização da versão de software;

b) Manutenção corretiva “on-site” (com reposição de peças e/ou equipamentos para os produtos de hardware);

c) Suporte técnico remoto.

1.5.3.A prestação dos serviços relacionados à garantia não deve imputar qualquer custo adicional ao TRE-MT;

1.5.4.A CONTRATADA deverá disponibilizar todas as atualizações dos softwares, *firmwares* ou microcódigos dos *hardwares* contratados, durante o período de garantia, sem ônus adicional;

1.5.5.Mesmo após o término do prazo da garantia, as licenças deverão permanecer em operação, ainda que sem a possibilidade de fazer atualizações, permitindo qualquer tipo configuração na solução e equipamentos;

1.5.6.Caso as condições de licenciamento dos softwares fornecidos sejam alteradas pelo fabricante durante o período de garantia, as funcionalidades e os quantitativos definidos não deverão ser prejudicados;

1.5.7.Caso a alteração na forma de licenciamento implique em perdas qualitativas e/ou quantitativas, licenças complementares deverão ser fornecidas ao TRE-MT sem custo adicional.

1.5.8.A CONTRATADA deverá notificar o fiscal do contrato sobre a descontinuidade dos produtos, objeto deste Termo de Referência, com antecedência mínima de 6 (seis) meses;

1.5.9.Quando o suporte resultar na necessidade de substituição de equipamentos, será responsabilidade da empresa contratada providenciar a troca perante a fabricante, as suas expensas e sem qualquer custo adicional para o Tribunal, responsabilizando-se, inclusive, pelo envio de pessoal até as dependências do prédio sede do TRE-MT, se necessário, para movimentação dos bens;

1.5.10.Será a empresa contratada quem responderá perante a União pelo cumprimento da contratação em qualquer hipótese;

1.5.11.Todas as licenças/autorizações deverão constar na conta do TRE-MT no site da fabricante ou em plataforma específica para este fim;

1.5.12.Durante o período de garantia contratual, a CONTRATADA deverá prover serviço de manutenço corretiva e de suporte técnico remoto para os produtos adquiridos;

a) A CONTRATADA deverá disponibilizar Central de Atendimento no Brasil para abertura de chamados de Assistência Técnica e implementações, na modalidade 24/7 (vinte e quatro horas por dia, em todos os dias da semana, inclusive feriados), indicando 0800 e/ou endereço de e-mail ou de site na Internet para abertura de chamado.

1.5.13.Entende-se por suporte técnico remoto as seguintes atividades para tratamento de problemas relacionados à solução:

a) Orientações sobre uso, configuração e instalação dos produtos adquiridos;

b) Questões sobre compatibilidade e interoperabilidade dos produtos adquiridos (hardware e software);

c) Orientações para identificar a causa de uma falha de software e/ou hardware;

d) Para os casos de defeitos de software conhecidos, devem ser fornecidas as informações sobre a correção ou a própria correção;

e) No caso de defeitos de software não conhecidos, a assistência técnica da CONTRATADA deverá enviar as informações sobre a falha ao fabricante do produto para que o mesmo forneça a solução. A CONTRATADA deverá informar o número do chamado aberto junto ao fabricante, bem como uma estimativa de prazo para solução da falha;

f) Orientação para solução de problemas de "*performance*" e "*tuning*" das configurações dos produtos adquiridos;

g) Orientação quanto às melhores práticas para implantação dos produtos de software adquiridos;

h) Apoio na recuperação de ambientes em caso de panes ou perda de dados;

i) Apoio para execução de procedimentos de atualização para novas versões dos produtos de software instalados.

1.5.14.Entende-se por manutenção corretiva a disponibilização de soluções destinadas a corrigir problemas originados por falhas de software e/ou hardware, incluindo o fornecimento de peças e/ou

equipamentos, atualização de versão, patches de correção, de configuração e demais procedimentos necessários objetivando o retorno do ambiente operacional;

a) A CONTRATADA obriga-se e compromete-se a não utilizar material de reposição improvisado. As peças e/ou equipamentos que vierem a ser substituídas deverão ser novos e originais do fabricante.

1.5.15.Durante o período de garantia contratual, os serviçs de manutenço corretiva serão prestados por técnicos devidamente habilitados e credenciados pela CONTRATADA, na modalidade “on-site”, ou seja, no local onde os equipamentos encontram-se instalados;

a) A partir da análise do fiscal do contrato, caso a manutenção remota não implique em redução da qualidade da solução, a mesma poderá ser autorizada.

1.5.16.A modalidade de atendimento deverá ser em regime 8x5 (8 horas por dia x 5 dias da semana);

1.5.17.O fato de qualquer um dos equipamentos relacionados neste Termo de Referecia não utilizar a ultima versão disponibilizada de quaisquer dos softwares instalados originalmente, incluindo *firmwares*, não poderá ser utilizado pela CONTRATADA como argumento para postergar eventual intervenço nos equipamentos, a menos que tenha sido objeto de notificação e que seja apresentada documentaço correlacionando a falha detectada com a versão de software instalada;

1.5.18.Deverão ser considerados os prazos apresentados na Tabela 2, estipulados de acordo om a severidade dos chamados de suporte técnico remoto e manutenção corretiva.

Severidade informada	Prazo de atendimento
1	4 horas corridas
2	24 horas corridas
3	72 horas corridas
4	48 horas corridas

Tabela 3. Prazos de atendimento.

1.5.19.Severidade 1, refere-se à ocorrência ou perda ou paralização de serviços, configurando-se como situação de emergência, possuindo uma ou mais das seguintes características:

a) Dados corrompidos;

b) Uma função crítica não está disponível;

c) O sistema se desliga repentinamente causando demoras excessivas e intermitências na utilização de recursos;

d) O sistema falha repetidamente após tentativas de reinicialização.

1.5.20.Severidade 2, refere-se à ocorrência de grave perda de funcionalidades em programas ou sistemas, inexistindo alternativas de contorno, sem, no entanto, interromper em sua totalidade a prestação do serviço;

1.5.21.Severidade 3, refere-se à ocorrência de perda, de menor relevância, de funcionalidades em programas ou sistemas, causando apenas inconveniências para o devido funcionamento das aplicações;

1.5.22.Severidade 4, refere-se necessidade de prestação de informaçes, aperfeiçamentos ou esclarecimentos sobre documentação ou funcionalidades de programas, porém, sem prejudicar diretamente a operaço das aplicaçes.

1.5.23.O nível de severidade será atribuído pela equipe técnica do TRE-MT no momento da abertura do chamado;

1.5.24.No atendimento dos chamados, para efeitos de apuraço do tempo gasto pela CONTRATADA para a disponibilização da solução, serão desconsiderados os períodos em que o TRE-MT estiver responsável por executar aces necessárias para a análise e solução da ocorrêcia;

1.5.25.Considerando que a solução das ocorrêcias de *software*, pela sua natureza, pode envolver atividades relacionadas ao desenvolvimento de *patches* específicos, admite-se para todos os casos a adoção de solução de contorno (*workaround*), respeitados os prazos definidos para cada severidade informada, sem prejuízo da disponibilização da solução definitiva cabível.

a) Nesse caso, a partir do encerramento do chamado original, com a disponibilização da solução de contorno, deverá ser imediatamente aberta uma nova ocorrência para provimento da solução definitiva, considerando os prazos estabelecidos na Tabela 3.

Severidade informada	Prazo de atendimento
1	15 dias corridos
2	30 dias corridos
3	45 dias corridos

Tabela 4. Prazos para a solução definitiva.

1.5.26.Considerando a solução de ocorrências de *hardware*, caso se esgote o prazo de atendimento solução da ocorrência, sem que seja sanado o defeito reclamado, a CONTRATADA deverá providenciar a substituição do equipamento ou módulo defeituoso por outro, em caráter definitivo, dentro do prazo máximo de 5 (cinco) dias corridos, contados a partir da expiração do prazo de atendimento e solução;

1.5.27.Para fins de cálculo de período decorrido para atendimento e solução da ocorrêcia de *software*, será contabilizado o prazo entre a formalizaço e o fechamento efetivo da ocorrêcia – seja essa solução de caráter definitivo ou provisório com a disponibilizaço de solução de contorno (*workaround*).

1.5.28.Para fins de cálculo de período decorrido para atendimento e solução da ocorrêcia de *hardware*, será contabilizado o prazo entre a formalizaço e o fechamento efetivo da ocorrêcia, ou seja, somente após a solução de caráter definitivo.

a) Nos casos em que o prazo para atendimento e solução da ocorrência não for cumprido e a CONTRATADA for obrigada a substituir o equipamento ou módulo defeituoso, a sanção pelo descumprimento do prazo para atendimento e solução da ocorrência será contabilizado até que a substituição tenha sido finalizada.

b) Para fins de cálculo de período decorrido para substituição do equipamento ou módulo defeituoso, será contabilizado o prazo após o esgotamento do prazo para atendimento e solução da ocorrência e a entrada em operação do novo equipamento ou módulo;

c) Entende-se como substituição do equipamento, ou módulo defeituoso, por outro em caráter definitivo, a desativação e remoção física do equipamento ou módulo defeituoso, seguida da ativação física e lógica do equipamento ou módulo substituído, reestabelecendo completamente o serviço que o equipamento atendia antes da ocorrência.

1.5.29.Independentemente da subscrição e garantia da fabricante da Solução, e dos itens adquiridos, a licitante será responsável pela intermediação dos pedidos de suporte da equipe técnica do Tribunal perante a fabricante. Isso posto, o Tribunal poderá abrir chamado perante a empresa contratada ou diretamente no site da fabricante (a seu exclusivo critério), cabendo à contratada na primeira hipótese, encaminhar os chamados à fabricante ou apresentar, ela própria, uma solução.

2. DO SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO (ITEM 2)

2.1. A contratada deverá realizar a instalação física de todo componente de *hardware* e *software*, incluindo sua configuração e interligação física (cabeamento) e lógica à rede de dados do TRE-MT;

2.2. A contrata deverá providenciar a aplicação de todas as correções e *upgrades* de *software* liberados até a data de instalação, incluindo atualizações de *firmware* dos componentes de *hardware* que compõem a solução;

2.3. O prazo para a conclusão da instalação da solução será de 30 (trinta) dias úteis, contatos a partir da emissão do Termo de recebimento:

2.3.1. Considerando as tratativas para combate a pandemia de COVID-19, o início da instalação poderá ser adiado, em comum acordo, mediante aprovação do Secretário de Tecnologia da Informação, desde que não gere custos adicionais para o TRE-MT.

2.4. Constatada a ocorrência de divergências na especificação técnica ou qualquer outro defeito de operação durante a instalação da solução, fica a CONTRATADA obrigada a providenciar a sua correção ou a substituição dos produtos adquiridos;

2.5. Caso sejam constatadas anormalidades ou detectados problemas, o TRE-MT comunicará formalmente os problemas detectados e que a instalação não foi concluída. A CONTRATADA terá prazo adicional de 10 (dez) dias úteis, contados a partir do dia seguinte à confirmação de recebimento da comunicação, para sanar os problemas/anormalidades detectados, sujeitando-se a CONTRATADA à s penalidades previstas;

2.6. Os serviços de instalação o deverão ocorrer em dias úteis, no horário compreendido entre 8:00hrs e 17:00hrs, salvo definição contrária, realizada em comum acordo entre o TRE-MT e a CONTRATADA;

2.6.1.Os serviços de instalação deverão ser agendados previamente com a equipe técnica do TRE-MT;

2.7. Os produtos adquiridos serão considerados instalados e o Termo de Aceite será emitido após a verificação da conformidade da instalação e da configuração, realizadas com as condições constantes neste Termo de Referência e que não existem anormalidades ou foram sanados todos os problemas detectados;

2.8. O TRE-MT terá o prazo de até 15(quinze) dias úteis para emitir o Termo de Aceite;

2.9. Correrá por conta da CONTRATADA toda e qualquer despesa, independente da sua natureza, decorrente dos serviços de instalação descritos;

2.10. O serviço de instalação deverá ser planejado e executado por profissionais qualificados e certificados oficialmente pelo fabricante:

2.10.1. É facultado a este TRE-MT solicitar documentação comprovando a certificação dos profissionais elencados para o processo de instalação.

2.11. Ao final da instalação, a CONTRATADA deverá repassar o conhecimento de toda a solução por um período mínimo de 16 (dezesseis) horas corridas, fornecendo relatório detalhado contendo todos os itens configurados no projeto (as-built), etapas de execução e toda informação pertinente a posterior continuidade e manutenção da solução implantada.

3. DA CAPACITAÇÃO (ITEM 3)

3.1. A empresa a ser contratada deverá fornecer capacitação oficial (treinamento), obedecendo o conteúdo oficial das provas de certificação da Fabricante;

3.2. A cada aquisição, a empresa contratada deverá indicar um calendário contendo as datas e as localidades de realização dos treinamentos nos 180 dias seguintes, sendo que:

3.2.1. O calendário deverá permitir pelo menos três datas para capacitação no período, distribuídas de maneira equidistantes, disponíveis em qualquer das capitais ou grandes centros urbanos do país;

3.2.2. O Tribunal poderá escolher qualquer das dadas de capacitação informada (ou mais de uma para pessoas distintas), desde que com antecedência mínima de 30 (trinta dias);

3.2.3. A não entrega ou indicação do calendário no prazo de 10 (dez) dias após o recebimento da nota de empenho, ou a entrega em desacordo com as especificações deste Termo de Referência, ensejara a sanção de multa na ordem de 0,5% (meio por cento) do valor total da contratação, limitada a 10 % do valor total, por dia de descumprimento.

3.3. A capacitação, com duração mínima de 40 (quarenta) horas, poderá ser dividida em até 3 (três) módulos, ministrados em datas diferentes, de acordo com o portfólio da fabricante, devendo conter, no mínimo, os seguintes conteúdos por módulo:

3.3.1. Gerenciamento e administração da solução:

a) Visão geral da solução, incluindo procedimentos de instalação, atualização e administração;

b) Ativação de licenças;

c) Provisionamento de módulos e *features*;

d) Configuração de interfaces e serviços essenciais de rede como NTP e DNS;

e) Alta disponibilidade e tolerância a falhas;

f) Monitoramento do ambiente e estado da solução;

g) Monitoramento de tráfego;

h) *Debug* na plataforma;

i) Logs.

3.3.2. Funcionalidade de balanceamento de carga

a) Balanceamento de carga e configuração na plataforma;

b) Persistência, incluindo cookies, SSL e SIP;

c) Monitoramento de aplicações;

d) Configuração da funcionalidade, incluindo alta disponibilidade;

e) *Debug*;

f) Logs

3.3.3. Funcionalidade de *Web Application Firewall*

a) Visão geral da funcionalidade e configuração na plataforma;

b) Vulnerabilidade em aplicações web;

c) Políticas de segurança;

d) Ajustes finos de políticas de segurança de aplicações web;

e) Identificação e prevenção dos principais ataques de aplicações web;

f) Monitoramento e relatórios;

g) Logs;

h) *Debug*;

i) Mitigação de ataques de força-bruta, DoS e bots.

j) Criptografia e segurança de dados

3.4. Será permitido à CONTRATADA subcontratar o treinamento de outra empresa que preste serviços para a Fabricante (ou à própria 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. O treinamento deverá ser ministrado por profissionais certificados como instrutores pela Fabricante;

3.6. O treinamento deve ser ministrado em português do Brasil. O material do treinamento deve ser preferencialmente em português. Caso não exista material oficial do produto em português, será aceito material em inglês. O material poderá ser em formato digital;

3.7. O treinamento deverá ocorrer em dias úteis, no horário comercial em centro especializado para este fim, salvo quando acordado de forma diferente entre a fiscalização e a empresa a ser contratada, observado em qualquer caso a vantajosidade para a administração pública a critério exclusivo desta Corte;

3.8. Os custos com deslocamento da equipe técnica do Tribunal para a cidade onde se realizará o treinamento (Centros Especializados de Treinamento) serão de responsabilidade desta Corte;

3.9. O certificado de conclusão do curso deverá ser emitido pela Fabricante ou pela empresa a ser contratada, ou ainda pela responsável legal pelo treinamento, se subcontratado;

3.10. A ausência do servidor ao treinamento é de responsabilidade do TRE-MT, cabendo a contratada informar no certificado a carga horária e assiduidade do servidor e em documento próprio, as ausências ou razões para inabilitação para recepção do certificado;

3.11. O cancelamento/adiamento de participação (unitária ou coletiva) deverá ser facultado ao Tribunal sem qualquer custo, desde que com antecedência mínima de 15 (quinze) dias da realização da capacitação;

3.12. O treinamento ofertado deve seguir o modelo padrão de capacitação disponível no mercado naquilo que couber.

Cuiabá, 14 de setembro de 2021.

Dr. Luís Cézar Darienzo Alves

Secretário de Tecnologia da Informação

Documento assinado eletronicamente por **LUIS CEZAR DARIENZO ALVES**, **SECRETÁRIO**, em 14/09/2021, às 18:20, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link " Verificador " informando o código verificador **0323949** e o código CRC **DC6D1F79**.