ESTUDOS TÉCNICOS / 2022 - SEINF

1. IDENTIFICAÇÃO DA SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO

SOLUÇÃO DE TI	
NOME DA SOLUÇÃO DE TI:	Aquisição de solução de Web Application Firewall (WAF)
ÁREA DEMANDANTE:	CODIN
E-MAIL DO DEMANDANTE:	rosemberg.maia@tre-pi.jus.br
TELEFONE DO DEMANDANTE:	86 2107-9762

2. DESCRIÇÃO DA SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO

A Tecnologia da Informação tornou-se para a administração pública, em especial o judiciário federal, ferramenta essencial para otimização das atividades administrativas, possibilitando a modernização da prestação jurisdicional, mediante a implantação de procedimentos mais ágeis, seguros, integrados e acessíveis aos jurisdicionados e ao cidadão. Tal fato decorreu da transformação digital, que nos últimos anos tem alavancado a digitalização dos processos de trabalho, proporcionando o alcance de diversas metas, consolidada em dois aspectos principais: a capacidade de lidar com o gigantesco número de informações, com o armazenamento e processamento de dados, recurso sem o qual o gerenciamento das informações já teria se tornado inviável e insustentável; e, em segundo lugar, por meio de tecnologias e sistemas de informação baseados na Web, que deram suporte à consecução da transparência e da razoável duração do processo legal por meio da digitalização dos processos de trabalho, assegurando a celeridade da tramitação processual, oferecendo como resultado a eficiente prestação jurisdicional. Os recursos, tecnologias e serviços computacionais, tornaram-se a base para a garantia da confiabilidade, integridade e disponibilidade das informações custodiadas.

Com a ampliação da disponibilização das soluções baseadas em serviços e protocolos que constituem a Web, principalmente, HTTP (*HyperText Transfer Protocol*) e HTTPS (*HyperTextTransfer 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. Entretanto, estes meios 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. Portanto, 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.

Deste modo, milhares de sites são invadidos todos os dias devido a configurações incorretas ou códigos vulneráveis. Neste contexto, estudos recentes apontam que cerca de 50% das aplicações Web disponíveis na Internet possuem pelo menos uma vulnerabilidade de alta criticidade, como SQL *Injection*. Se for levado em consideração o nível de risco médio, cerca de 90% das aplicações publicadas na Web podem ser consideradas vulneráveis (***Web Application Vulnerability Report***, 2019). Ainda segundo relatórios especializados, a vulnerabilidade de *Cross-Site Scripting* (XSS) é uma das mais comuns e mais exploradas (representando cerca de 30%) em aplicações Web (***The HackerOne Top 10 Most Impactful and Rewarded Vulnerability Types*** , 2019). Além de ser frequente, em alguns casos, a exploração da vulnerabilidade XSS permite ao atacante acessar recursos e dados privados. Além das vulnerabilidades conhecidas, existem ainda as chamadas falhas do tipo "*Zero Day*", que se trata de uma vulnerabilidade de segurança desconhecida do público e do próprio desenvolvedor de um software. Isso significa que, a partir do momento em que a falha é detectada, o fabricante do software tem efetivamente “zero dias” para produzir uma atualização que corrija o problema, impedindo a exploração por criminosos antes da aplicação do patch que corrige a vulnerabilidade. Por outro lado, por motivos, algumas vezes, intrínsecos ao código da aplicação, não é possível aplicar o patch sem a necessidade de reescrever parte ou todo o sistema. Portanto, existe a necessidade de adoção de mecanismos para mitigação do risco de ataques, enquanto a equipe de desenvolvimento está realizando ajustes na aplicação para possibilitar a aplicação do patch.

Como uma forma de contribuir para o estudo e proteção dos ambientes no cenário crítico das aplicações Web disponíveis na Internet, especialistas em segurança da informação criaram a fundação OWASP (*The Open Web Application Security Project*). A entidade tem como principal objetivo disseminar conhecimento sobre segurança de aplicações Web disponíveis na Internet. Além disso, a OWASP também mantém um ranking tri-anual das 10 vulnerabilidades mais recorrentes em sistemas Web, conhecido como OWASP Top 10

Objetivando mitigar o risco de ataques cibernéticos, por meio da estratégia de diminuição da superfície de ataque, uma das ferramentas que tem sido utilizada na proteção de aplicações Web é o *Web Application Firewall* (WAF). Um WAF é um serviço de segurança implementado entre o cliente (e.g., navegador/browser) e a aplicação (e.g., sistema PHP rodando num servidor Web Apache). A função do WAF é interceptar, inspecionar e processar as requisições entre o cliente e a aplicação. A partir de um conjunto de regras, ele classifica as requisições em maliciosas (que são geralmente bloqueadas) e não-maliciosas, isto é, que são encaminhadas até a aplicação. Apesar de ser um estratégia de proteção conhecida há alguns anos, a importância dos WAFs tem crescido rapidamente no contexto atual, onde ciber ataques, que exploram as vulnerabilidades mais recorrentes de aplicações Web, têm crescido exponencialmente.

Atualmente, a arquitetura de segurança implantada na maioria dos Tribunais Eleitorais está baseada principalmente em Firewall NG (*Next Generation*) e firewalls tradicionais. Firewall NG (*Next Generation*) realizam inspeção profunda de pacotes (verificação do conteúdo do pacote de dados), podendo incluir outras tecnologias, como os Filtros de URFs e sistemas de prevenção contra invasão (IPSs), que trabalham para interromper automaticamente os ataques contra a rede. Além disso, outros TREs também utilizam soluções baseadas em *endpoint*, como soluções de antivírus. A referida arquitetura vem até agora atendendo às necessidades básicas, no entanto, apresenta restrições quanto à capacidade e proteção de aplicações em camada 7. Resta claro, portanto, a necessidade de adequação da

infraestrutura às novas ameaças digitais, sobretudo frente ao número de acessos e ampliação dos serviços externos providos pela Justiça Eleitoral.

3. MOTIVAÇÃO / JUSTIFICATIVA

Com base nas diretrizes firmadas 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.

Dessa forma, visando ao alinhamento estratégico e ganho em escalabilidade, disponibilidade, confiabilidade na entrega dos serviços prestados à sociedade, o TRE-PI pretende adquirir solução de *Application Delivery Controller* (ADC) que compreende funções de balanceamento de aplicações e tráfego e firewall de aplicações.

Como dito acima, uma das funções realizada pela referida solução é o balanceamento de aplicações, responsável por realizar a distribuição das requisições em dois ou mais servidores ou entre Datacenters. Objetiva a otimização de recursos, maximização do desempenho e minimização do tempo de resposta das aplicações corporativas para usuários internos e clientes externos.

Outra função que pode ser realizada pelo ADC é o de firewall de aplicações (mecanismo de segurança - WAF), que aumentará a disponibilidade dos sistemas essenciais, acrescendo uma série de funcionalidades à segurança de TIC do TRE-PI, mapeando acessos específicos que acontecem na camada de aplicação, com o objetivo de garantir a proteção adequada aos sistemas e dados armazenados no DataCenter do Tribunal.

Propõe-se, para tanto, a aquisição de Solução de Segurança da Informação – *Application Delivery Controller* (ADC) com função de Firewall de Aplicação Web (WAF), visando à segurança e o 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, consequentemente, 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.

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 judiciários, 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.

4. RESULTADOS ESPERADOS

- Garantir que o acesso lógico aos ativos seja gerenciado e protegido, por meio de mecanismos de segurança de perímetro;
- Tornar a infraestrutura da Justiça Eleitoral mais segura e confiável;
- Prover resiliência ao ambiente de produção;
- Assegurar a redundância adequada ao acesso de Sistemas hospedados pelo Tribunal.

5. REQUISITOS DE NEGÓCIO

5.1 – Requisitos funcionais (Necessidades de negócio)

NECESSIDADE 1				
Proteção de servidores que hospedam aplicações WEB				
ID	**FUNCIONALIDADE**	**ID**	**RESPONSÁVEL**	**ÁREA**
1	Inspeção SSL	1	Área demandante	CODIN
2	Decriptografia do tráfego SSL em hardware dedicado	1	Área demandante	CODIN

NECESSIDADE 2				
Balanceamento de carga				
ID	**FUNCIONALIDADE**	**ID**	**RESPONSÁVEL**	**ÁREA**
1	Balanceamento de carga por: *hash*, *persistent hash*, *least connections*, *least connections per service*, *round-robin*, *response time* e *bandwitch*	1	Área demandante	CODIN

2	Balanceamento por conteúdo HTTP utilizando: URL *hostname*, URL *path*, URL *page name*, URL *page type*, cabeçalho HPPT e texto específico	1	Área demandante	CODIN

NECESSIDADE 3				
Monitoramento e detecção de ataques				
ID	**FUNCIONALIDADE**	**ID**	**RESPONSÁVEL**	**ÁREA**
1	Proteção de aplicações WEB contra ameaças registradas no OWASP *Top Ten Vulnerabilities*	1	Área demandante	CODIN
2	Proteção contra ataques conhecidos e *Zero Day*	1	Área demandante	CODIN
3	Proteção contra ataques DDoS	1	Área demandante	CODIN

NECESSIDADE 4				
Redução da superfície de ataques cibernéticos da Justiça Eleitoral				
ID	**FUNCIONALIDADE**	**ID**	**RESPONSÁVEL**	**ÁREA**
1	Proteção contra ataques em camada de aplicação WEB, como: XSS, SQL *Injections*, OS *command injections*, *Sensitive information leakage*, CSRF, *Application* Dos, etc	1	Área demandante	CODIN
2	Visibilidade SSL/TLS	1	Área demandante	CODIN

5.2 – Requisitos não-funcionais

ID	TIPO	REQUISITO
		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. 1. O treinamento deverá oferecer carga horária total de no mínimo 20(vinte) horas. 2. Serão aceitos apenas treinamentos nas modalidades online ao vivo (EAD), podendo os treinamentos online ao vivo serem gravados, a critério da CONTRATANTE. 3. A CONTRATADA deve prover capacitação técnica em turma com no mínimo 5 (cinco) e no máximo 8 (oito) participantes. 4. Se o treinamento for ofertado na modalidade EAD, deverá respeitar o limite de 4 (quatro) horas por dia. 5. O treinamento deverá cobrir conhecimentos necessários para instalação, administração, configuração, gerência, otimização, resolução de problemas e utilização da solução. As despesas decorrentes do serviço de treinamento (instrutores, confecção do material didático, licenciamento de plataforma de videoconferência etc.) serão de exclusiva responsabilidade da CONTRATADA. O treinamento poderá ser composto de mais de 1(um) módulo, que deverão ser discriminados na proposta da licitante. 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 noite m (e) anterior. O Tribunal poderá planejar e escolher qualquer das datas, ou períodos, dos eventos de capacitação no prazo de validade da ata de registro de preços, a contar da entrega do calendário.

1	Requisitos de capacitação	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. 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. 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. 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. O treinamento deve ser ministrado em português do Brasil. Caso não exista material oficial do produto em língua portuguesa, será aceito material em inglês. O treinamento deverá oferecer acesso a laboratório prático virtual, fornecido pela contratada, para configuração e execução de exercícios práticos. • 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. 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. A ausência do servidor ao treinamento é de responsabilidade do Tribunal, cabendo a contratada informar no certificado a carga horária e assiduidade do servidor. A Contratada deverá aplicar o Formulário de Satisfação, conforme modelo de formulário constante no Anexo III deste Termo de Referência. 1. 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 considerado proveitoso. 2. 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) itens avaliados; 3. Caso o resultado da Avaliação de Instrutor seja considerado “não proveitoso”, o treinamento fornecido será considerado não aceito; 4. 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; 5. Na hipótese de o resultado do segundo treinamento ser “não proveitoso”, o objeto será considerado não aceito, aplicando-se as sanções previstas contratualmente.

2	Requisitos Legais	A CONTRATADA deve observar o cumprimento de todas as leis e normas aplicáveis ao OBJETO, em especial atenção àquelas relacionadas ao pagamento das obrigações empresariais relacionadas à encargos fiscais, trabalhistas e previdenciários. Outras Referências: • Resolução TRE-PI nº 458/2022, que dispõe sobre a Política de nivelamento, atualização e renovação da infraestrutura de Tecnologia da Informação no âmbito da Justiça Eleitoral do Piauí; • Resolução CNJ n° 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 n° 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 - SISP, do Poder Executivo federal.
		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; 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; 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; 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; 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; Suporte Técnico durante o período de Garantia Técnica: • 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; • 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; • 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; A CONTRATADA deverá entregar no protocolo do CONTRATANTE, mensalmente, até o 5° (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:

3	Requisitos de Manutenção	• 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; • Cada chamado técnico aberto será avaliado individualmente pelo Gestor do Contrato; • 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; • 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. 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. 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 em danos físicos e lógicos aos equipamentos, sem que isto possa ser usado como pretexto pela CONTRATADA para se desobrigar do suporte da solução. 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. 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. 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; 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. As atualizações e correções (patches) do software e firmwares deverão estar disponibilizados via WEB ou fornecidas em mídia (CD ou DVD), quando desta forma forem solicitadas. 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. 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.

4	Requisito Temporal	Deverá ser realizada após a assinatura do Contrato, uma reunião de alinhamento remota, com o objetivo de alinhar as expectativas, nivelar os entendimentos acerca das condições estabelecidas no Contrato, Edital e em seus Anexos, e esclarecer possíveis dúvidas acerca do objeto, conforme agendamento efetuado pelo Gestor do Contrato, bem como: • Apresentar a relação do pessoal técnico especializado, adequado e disponível para a execução do objeto deste Estudo, bem como a qualificação de cada um dos membros da equipe técnica. • Apresentar a declaração de disponibilidade, assinada por cada integrante da equipe técnica mencionada na alínea anterior, bem como o Termo de Confidencialidade da Informação. • Apresentar um cronograma para implantação e configuração da Solução adquirida, o qual deverá sofrer aval do Gestor do Contrato. • Apresentar a logística para realização do treinamento da Solução adquirida. • Os profissionais indicados pela CONTRATADA deverão efetivamente implantar e configurar a Solução objeto deste Estudo, admitindo-se suas substituições por profissionais de experiência equivalente ou superior, desde que aprovada previamente pelo órgão. • O prazo para a entrega da solução será de até 90 (noventa) dias consecutivos, contados a partir do primeiro dia útil após a confirmação de recebimento da Ordem de Fornecimento emitida pela Fiscalização do Contrato. • O prazo de implantação da solução será de até 30(trinta) dias consecutivos a partir do recebimento do objeto.
5	Requisitos de Segurança da Informação	A Contratada deverá submeter-se aos procedimentos de segurança existentes, ou que possam ser criados durante a vigência do contrato. Os procedimentos deverão ser observados sempre que for necessária a presença nas dependências da Contratante. A empresa contratada deverá respeitar as diretrizes constantes da Política de Segurança da Informação do da Justiça Eleitoral (Resolução TSE No 23.501/2016), obrigando-se a manter sigilo a respeito de quaisquer informações, dados, processos, fórmulas, códigos, cadastros, fluxogramas, diagramas lógicos, dispositivos, modelos ou outros materiais de propriedade do Tribunal Regional Eleitoral do Piauí, e de outros partícipes desta contratação, aos quais tiver acesso em decorrência do objeto da presente contratação, ficando terminantemente proibida de fazer uso ou revelação destes sob qualquer justificativa; O Tribunal Regional Eleitoral do Piauí terá propriedade sobre todos os documentos e procedimentos operacionais produzidos no escopo da presente contratação; Os documentos eventualmente produzidos deverão ser repassados ao Tribunal tanto em formato não editável (PDF) como também em formato editável (.DOCX). O fornecedor assinará, no ato da entrega das licenças e do serviço, Termo de Confidencialidade, em que se comprometerá a não acessar, não divulgar e proteger todos os dados de infraestrutura e de vulnerabilidades do contratante a que tiver acesso, que abrangerá todos os seus colaboradores e terceiros, sob as penas da lei.
6	Requisitos Sociais, Ambientais e Culturais	A documentação e os manuais da solução deverão, preferencialmente, ser apresentados no idioma Português (Brasil), eventualmente poderão ser apresentados em inglês. Todos os contatos para gerenciamento de chamados e suporte técnico deverão ser realizados em Português (Brasil). O licenciamento e o suporte devem ser prestados preferencialmente no idioma português do Brasil. 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. 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.
7	Requisitos de Desempenho	Não se aplica

5.3 – Requisitos tecnológicos

ID	TIPO	REQUISITO
		Especificações técnicas mínimas: 1. Os *appliances* físicos devem ser novos e de primeiro uso; 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 nas Especificações técnicas mínimas.

3. Devem ser novos, sem uso prévio e entregues em perfeito estado de funcionamento. Não devem ser remanufaturados, recondicionados ou possuir reparos de qualquer espécie.
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.
5. As funcionalidades da solução (balanceador de carga, *global server load balancing*, proteção para aplicação, proteção contra ataque DDoS, DNS *Application Firewall*, inspeção SSL etc) deverão ser licenciadas pelo período de 60 (sessenta) meses;
6. O equipamento será instalado em rack com largura padrão de 19 polegadas, padrão EIA-310, ocupando no máximo 2Us do referido rack;
7. 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;
8. Deve ser fornecido com todos os cabos de ligação lógica e elétrica necessários à instalação e perfeito funcionamento.
9. Dispor de fonte de alimentação redundante com tensão de entrada de 110V a 220V AC automática e frequência de 60Hz;
10. Possuir sistema operacional customizado especificamente para funções de *Web Application Firewall*, não podendo ser entregue *appliance* do tipo NGFW;
11. 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);
12. Possuir 01 interfaces 1GE, incluso interfaces de gerência com conectores padrão RJ45;
13. Todas as interfaces fornecidas devem estar licenciadas e habilitadas para uso imediato;
14. Possuir no mínimo de 8.000 Mbps de *throughput* em camada 7;
15. Possuir capacidade de 4.000 transações por segundo (TPS) em TLS padrão RSA (chaves de 2.048 bit). Serão aceitos os equipamentos que apresentarem a mesma quantidade de conexões por segundo;
16. Recursos de agregação de portas baseado no protocolo LACP, segundo o padrão IEEE 802.3ad;
17. Memória RAM mínima de 16 GB;
18. Disco rígido com capacidade de armazenamento interno e retenção de logs para análise com capacidade mínima de 240GB;
19. Deve vir acompanhado de todas as licenças de software ou hardware necessárias para atendimento das funcionalidades exigidas neste caderno de especificações técnicas;
20. Todas as funcionalidades devem continuar ativas, mesmo após o término do termo de garantia e suporte técnico;
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;
22. Suportar e garantir a instalação em ambiente de alta disponibilidade;
23. Deve permitir a configuração da solução em alta disponibilidade, permitindo o funcionamento em cluster do tipo ativo-passivo e ativo-ativo;
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;
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;
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;
27. O equipamento deve permitir a sincronização das configurações de forma automática;
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;
29. Possuir capacidade para gerenciar os recursos disponíveis de acordo com as funções habilitadas nos equipamentos SLB, GSLB,WAF, etc;

30. Fornecer recurso para o transporte de múltiplas VLANs por uma única porta (ou por um conjunto agregado de portas) utilizando o protocolo 802.1q;
31. Analisar e proteger tráfego HTTP/1.0, HTTP/1.1, HTTP/2.0 e/ou HTTP/3;
32. Possuir suporte a IPv6;
33. 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;
34. Deve suportar, no mínimo, 1.000 VLANs simultaneamente;
35. Implementar o SNTP (*Simple Network Time Protocol*) ou NTP (*Network Time Protocol*);
36. Possuir suporte à funcionalidade de VXLAN, essencial para integração com o ambiente de virtualização (*Software Defined Network*);
37. Assinar *cookies* digitalmente e editar endereços de URL ("*URL Rewriting*");
38. O equipamento deverá permitir a sincronização das configurações:
    a. De forma automática;
    b. Manualmente, forçando a sincronização apenas no momento desejado.
39. Permitir a configuração das interfaces de alta disponibilidade do cluster (*heartbeat*), com opções para:
    a. Compartilhar a rede de *heartbeat* com a rede de dados;
    b. Utilizar uma rede exclusiva para o *heartbeat*.
40. Permitir que regras customizadas em linguagem aberta possam ser utilizadas para customizar a distribuição dinâmica de tráfego e aumentar a proteção contra ataques;
41. 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;
42. Permitir a criação de políticas através de interface gráfica web ou CLI para manipulação de tráfego através de lógica para pelo menos os seguintes operadores:
    a. GEOIP, http-basic-auth, http-cookie, http-header, http-host, http-method, http-referer, http-set-cookie, http-status, http-uri e http-version
43. 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;
44. Deve implementar configuração de endereçamento IP estático ou dinâmico (DHCP/BOOTP) para a interface de gerenciamento;
45. Permitir acesso *in-band* via SSH;
46. Possuir console de administração com interface gráfica remota segura atendendo os seguintes requisitos:
    a. Permitir a definição de diferentes níveis de administração, no mínimo, um nível completo e outro somente de visualização de configurações e logs;
    b. Permitir a replicação de configurações e a aplicação de atualização de softwares para os elementos dos nós do cluster;
47. Manter internamente múltiplos arquivos de configurações do sistema;
48. Utilizar SCP ou HTTPS como mecanismo de transferência de arquivos de configuração e Sistema Operacional;
49. Os usuários de gerência deverão poder ser autenticados em bases remotas. No mínimo RADIUS, LDAP e TACACS+ deverão ser suportados;
50. Deverá ser possível associar aos usuários de bases externas como RADIUS, LDAP e TACACS+ o nível de acesso;
51. Possuir Interface Gráfica via Web;
52. Possuir auto-complementação de comandos na CLI;
53. Possuir ajuda contextual;
54. A Solução deve ter a capacidade de permitir a criação de MIBs customizadas ou ter suporte a snmpv1/v2/v3 para monitoramento do equipamento;
    a. A solução deve possuir arquivo de MIBS e documento descrevendo os OIDs e o que é possível coletar utilizando SNMP;
55. A Solução deve ter suporte a sFlow;
56. Interface por linha de comando (CLI – *Command Line Interface*) que possibilite a configuração dos equipamentos;
57. Possuir, no mínimo, 3 (três) níveis de usuários na GUI – Super-Usuário,

Usuário com permissões reduzidas, e usuário Somente Leitura;

58. 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;
59. A interface gráfica deverá permitir a configuração de qual partição o equipamento deverá dar o boot;
60. Possuir um comando, via CLI, que mostre o tráfego de utilização das interfaces (bps e pps);
61. Suportar a rollback de configuração salva e imagem;
62. Possuir e fornecer geração de mensagens de syslog para eventos relevantes ao sistema;
63. Possuir configuração de múltiplos syslog servers para os quais o equipamento irá enviar as mensagens de syslog;
64. Possuir armazenamento de mensagens de syslog em dispositivo interno ao equipamento;
65. A interface Gráfica deverá permitir a reinicialização do equipamento;
66. Reinicialização do equipamento por comando na CLI;
67. Possuir recurso de gerência via SNMP e implementar SNMPv1, SNMPv2c e SNMPV3;
68. Possuir traps SNMP;
69. Caso a solução possua suporte a RMON, deverá possuir suporte a monitoramento utilizando pelo menos 4 grupos: *statistics*, *history*, *alarms* e *events*;
70. Os logs de sistema devem ter a opção de ser armazenados internamente ao sistema ou em servidor externo;
71. Implementar *Debugging*: CLI via console e SSH;
72. Permitir a criação de políticas diferenciadas por aplicação e por URL, onde cada aplicação e URL poderão ter políticas totalmente diferentes;
73. Permitir a criação de políticas diferenciadas por aplicação;
74. 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;
75. Restringir métodos HTTP/ HTTPS permitidos, tipos ou versões de protocolos, tipos de caracteres e versões utilizadas de *cookies*;
76. Permitir as seguintes opções de implementação:
    a. Monitoramento (sem bloqueio);
    b. Proxy (reverso e transparente).
77. Permitir que novas políticas fiquem apenas monitorando o tráfego, sem bloqueá-lo, indicando caso aconteça algum evento;
78. Remover as mensagens de erro do conteúdo que será enviado aos usuários;
79. Em modo “monitoramento” (sem bloqueio), realizar análise e avaliação do tráfego, gerar relatórios com os dados analisados e simular bloqueios para efeito de avaliação;
80. 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;
81. Bloquear ataques aos servidores de aplicação, por meio dos seguintes recursos:
    a. Identificação, isolamento e bloqueio de ataques sofisticados sem impactar nas transações das aplicações;
82. Possuir proteção para XML integrado com suporte a filtro e validação de funções XML específicas da aplicação, tais como, por exemplo: *format check*, *limit check*, *sql injection check* e *cross-site scripting check*;
83. Com a finalidade de proteger as aplicações, a solução deve suportar proteções a JSON;
84. 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;
85. Quando detectada uma tentativa de ataque bloquear de imediato o tráfego ou a sessão;
86. Bloqueio com intermediação e interrupção da conexão;
87. Criação de políticas automáticas que bloqueiam o endereço IP que realizar violações;
88. Utilização de página HTML informativa e personalizável como HTTP Response

aos bloqueios;

89. Configuração de políticas de bloqueio baseadas em requisição HTTP, endereço IP e usuário de aplicação;
90. Identificar e armazenar o ataque acontecido com detalhes, com as seguintes informações:
    a. Endereços IP que originaram os ataques;
    b. Horário do ataque;
    c. Nome do ataque;
    d. Qual campo foi atacado;
    e. Quantas vezes esse ataque foi realizado;
91. Possuir mecanismo de aprendizado automatizado capaz de identificar todos os conteúdos das aplicações;
92. O perfil aprendido de forma automatizada pode ser ajustado, editado ou bloqueado;
93. Identificar ataques baseados em:
    a. Regras;
    b. Perfis de utilização;
    c. Assinaturas e/ou comportamento.
94. Deve possuir tecnologia para mitigação de DDoS em camada 7 baseado em analise comportamental, usando o aprendizado;
95. A solução deve possuir a capacidade de capturar tráfego no formato TCP Dump permitindo uma análise mais aprofundada por parte do administrador;
96. Detectar ataques de força bruta por meio dos seguintes métodos:
97. Aumento do tempo de resposta da aplicação monitorada ou bloqueio temporário do atacante;
98. Quantidade de transações por segundo (TPS), monitorando a quantidade de transações por segundo por endereço IP;
99. Detectar ataques do tipo força bruta em que:
    a. O atacante solicita repetidamente o mesmo recurso;
    b. O atacante realiza repetidas tentativas não autorizadas de acesso;
    c. São utilizados ataques automatizados de login.
100. Detectar ataques do tipo força bruta que explorem:
    a. Controles de acesso da aplicação (Erro 401 – *Unauthorized*);
    b. Solicitações repetidas ao mesmo recurso, em qualquer parte/URL da aplicação;
    c. Aplicações WEB que não retornam o Erro 401 (por meio da identificação de expressão regular no retorno/página de erro da aplicação);
    d. Gerenciamento de sessão (muitas sessões de um único endereço IP ou a um *range* de IPs);
    e. Clientes automatizados (robôs, requisições muito rápidas);
    f. Permitir a criação de políticas diferenciadas por aplicação e por URL, onde cada aplicação e URL poderão ter políticas totalmente diferentes;
    g. 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;
101. Apresentar proteção contra-ataques, como:
    a. *Brute Force Login*;
    b. *Buffer Overflow*;
    c. *Cookie Injection*;
    d. *Cookie Poisoning*;
    e. *Cross Site Request Forgery* (CSRF);
    f. *Cross Site Scripting* (XSS);
    g. *Server Side Request Forgery* (SSRF)
    h. *Directory Traversal*;
    i. HTTP *Denial of Service*;
    j. *Malicious Robots*;
    k. *Parameter Tampering*;
    l. *SQL Injection*;
    m. Web *Services* (XML) *attacks*;

1	Requisitos da Arquitetura Tecnológica	102. Permitir configurar granularmente, por aplicação protegida, restrições de métodos HTTP permitidos, tipos ou versões de protocolos, tipos de caracteres e versões utilizadas de *cookies*; 103. Suportar os seguintes critérios de decisão para realizar bloqueio ou gerar alerta, sendo que uma política pode conter um ou mais critérios simultaneamente: a. Assinatura de ataque ou IPs de atacantes conhecidos; b. Código de *response*; c. Conteúdo da *cookie*; d. Conteúdo do cabeçalho; e. Conteúdo do *payload*; f. *Hostname*; g. IP de origem; h. Método HTTP; i. Número de ocorrências em determinado intervalo de tempo; j. Parâmetro; k. *User-agent* (navegador); 104. Deve proteger contra os seguintes ataque: a. Ataques de negação de serviços automatizados; b. *Worms* e vulnerabilidades conhecidas; c. *Requests* em objetos restritos; 105. Deve proteger contra ataques SSRF (*Server Side Request Forgery*); 106. A solução oferecida deverá possuir proteção contra ataques, disponibilizando acesso a base de assinaturas e/ou atualizações periódicas até o fim do contrato; 107. Ao atualizar ou adicionar uma nova configuração na política de proteção de WAF, a solução deve possuir opção de colocar a regra ou aplicação em modo "*staging*" ou "*passive*" para evitar falsos positivos e não bloquear tráfego válido; 108. Deve permitir que possa ser especificado na política os tipos de arquivos que serão bloqueados (*File Types*); 109. A solução deve permitir a inspeção de *upload* de arquivos para os servidores de aplicação, ou enviar para inspeção através do protocolo ICAP; 110. Deve possuir uma proteção proativa comportamental contra ataques automatizados por robôs e outras ferramentas de ataque; 111. Ao detectar uma condição de DDoS, assinaturas dinâmicas devem ser automaticamente criadas e implementadas em tempo real para proteção da aplicação; 112. A solução deve possuir proteção de DDoS L7 baseado em análise comportamental, sem precisar de nenhuma configuração manual; 113. Possuir método de mitigação de DoS L7 baseado em: a. Descarte de todas as requisições de um determinado IP e/ou país suspeito; b. Defesa proativa contra Bot, através da injeção de um desafio no Browser ou via Javascript para detectar se é um usuário legítimo ou robô; 114. Aprender o comportamento da aplicação: a. Campos, valores e URLs; 115. Políticas sugeridas somente devem ser aplicadas após um período configurável ou possibilidade de aplicá-las posteriormente; 116. Inspecionar 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*; 117. 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; 118. Proteger contra mensagens XML e SOAP malformadas; 119. Utilizar o campo HTTP X-*Forwarded-For* sem modificar seu conteúdo de origem, permitindo a diferenciação em ambientes com NAT; 120. Remover as mensagens de erro do conteúdo que será enviado aos usuários; 121. 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; 122. Deverá permitir o cadastro de robôs que podem acessar a aplicação;

123. Deverá implementar proteção ao JSON (JavaScript Object Notation);
124. 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;
125. 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;
126. Deve proteger informações sensíveis e confidenciais da interceptação por terceiros, através da criptografia de dados. Deve proteger esses dados criptografados de *malwares* e *keyloggers*;
127. 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;
128. A solução deve fornecer relatórios consolidados de ataques com pelo menos os seguintes dados:
    a. 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.
129. Deverá permitir o agendamento de relatórios a serem entregues por e-mail;
130. Emitir os seguintes relatórios gráficos dos ataques por:
    a. Política de segurança;
    b. Tipos de ataques;
    c. Violações;
    d. URL que foram atacadas;
    e. Endereços IP de origem;
    f. Localização geográfica dos endereços IPs de origem;
    g. Severidade;
    h. Código de resposta;
    i. Métodos;
    j. Protocolos;
    k. Sessão;
131. Permitir a seleção de período para emissão dos relatórios;
132. Permitir a geração das seguintes informações, por período:
    a. Permitir auditoria detalhada das alterações de configuração efetuadas, indicando usuário, ação e horário;
    b. Informações estatísticas de quantidade de conexões completadas e bloqueadas;
    c. Informações estatísticas de fluxo de tráfego;
133. Identificação, isolamento e bloqueio de ataques sofisticados para os protocolos: HTTP e HTTPS;
134. 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;
135. 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;
136. 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;
137. 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;
138. A solução deve possuir 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:
    a. SSL *session cache timeout*;
    b. *Session ticket*;
    c. OCSP (*Online Certificate Status Protocol*) *Stapling*;
    d. *Perfect forward secrecy*;

139. 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:
    a. 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;
    b. 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;
    c. Ao realizar inspeção, proteção, *offload* e aceleração de tráfego criptografado através de SSL/TLS;
    d. 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;
140. Deve possibilitar a customização da interface gráfica da página de login;
141. 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:
    a. *Single Sign-on*:
        i. 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;
        ii. 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;
    b. VPN-SSL:
        i. 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;
        ii. 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;
        iii. modo “Network”, onde um usuário se conecta efetivamente à rede interna, obtendo um endereço IP roteável pela rede interna;
        iv. 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;
        v. Deverá ser compatível para Microsoft Windows, Linux, dispositivos/ baseados em Android e iOS e MAC OSX;
    c. 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;
142. Deve suportar autenticação de múltiplos fatores utilizando *tokens* de Hardware ou *One-Time Passcode* (OTP);
143. Deve possuir capacidade para realizar proxy reverso com a finalidade de omitir a URI real, promovendo assim o acesso seguro às aplicações web internas;
144. Melhora da disponibilidade das aplicações através do balanceamento da entrada de tráfego deve possuir, ao menos, as seguintes características:
    a. DNS autoritativo;
    b. DNS secundário;
    c. DNS resolver;
    d. DNS cache;
    e. Balanceamento de DNS servers;
    f. DNSSec;
145. Capacidade de uso de chave criptográfica para comunicação segura entre servidores DNS;
146. A solução deve realizar o *offload* dos servidores de DNS, funcionando como o DNS secundário;
147. A solução deve suportar pelo menos os seguintes tipos de requisição DNS: SOA, A, AAAA, CNAME, MX,NS, PTR, SRV, TXT;
148. Deve ser capaz de gerar estatísticas sobre consultas de DNS por: aplicação, nome da *query*, tipo da *query*, endereço IP do cliente;

149. Deve ser possível configurar a solução de modo *inline* a estrutura de DNS existente e transparente sem requerer grandes mudanças na infraestrutura;
150. Deve prover as respostas a *queries* DNS da própria RAM CACHE;
151. A solução deve ser capaz de realizar IP *Anycast*;
152. A solução deve ser capaz de realizar DNSSec, independente da estrutura dos servidores DNS em uso;
153. A solução de alta disponibilidade não deve depender de BGP ou outro protocolo de roteamento;
154. A solução deve suportar, no mínimo, os seguintes métodos de balanceamento:
    a. *Round Robin*;
    b. *Global Availability*;
    c. Geografia;
    d. *Least Connections*;
155. A solução deve ser capaz de lidar com clientes IPv6 quando o site atende apenas com IPv4 (requests AAAA ou A6);
156. A solução deve suportar *edns-client-subnet* (ECS) para tanto responder requisições de clientes ou encaminhar requisições de clientes (*screening*);
157. Possuir recursos para executar compressão de conteúdo HTTP, para reduzir a quantidade de informações enviadas ao cliente;
158. Possuir no mínimo um dos tipo de compressão a seguir: gzip1 a gzip9 ou *deflate*;
159. Possuir capacidade para definir compressão especificamente para certos tipos de objetos;
160. Permitir o balanceamento de aplicações em um *pool* de servidores, independentemente do hardware, sistema operacional e tipo de aplicação;
161. A solução deve permitir aplicar criptografia de cookies para a proteção dos cookies utilizados pela aplicação web;
162. Possuir recursos para balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência de sessão dos seguintes tipos:
    a. Por cookie;
    b. Endereço de origem;
    c. Sessão SSL;
    d. Através de qualquer parâmetro do cabeçalho HTTP;
    e. Através da análise do SIP Call ID ou *Source* IP;
163. O equipamento oferecido deverá possuir monitores predefinidos ou possibilitar a configuração para, no mínimo, os seguintes protocolos:
    a. ICMP, HTTP, HTTPS, Diameter, FTP, SASP, SMB, RADIUS, MSSQL, NNTP, ORACLE, RPC, LDAP, IMAP, SMTP, POP3, SIP, Real Server, SOAP, SNMP e WMI;
164. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor;
165. Realizar *Network Address Translation* (NAT);
166. Realizar proteção contra *syn flood*;
167. Realizar as proteções de cabeçalho: X-Frame-Options, X-XSS-Protection, X-Content- Type- Options;
168. Permitir espelhamento do trafego, 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;
169. 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;
    a. 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;
    b. 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;
170. 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; 171. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor real; 172. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor virtual; 173. Possuir recursos para limitar o número de sessões estabelecidas com cada grupo de servidores; 174. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor físico; 175. Realizar *Network Address Translation* (NAT); 176. Realizar proteção contra *Denial of Service* (DoS); 177. Realizar proteção contra *Syn flood*; 178. Realizar limpeza de cabeçalho HTTP; 179. Deve possuir suporte a *Link Layer Discovery Protocol* (LLDP); 180. Suporte a otimização do protocolo TCP para ajustes a parâmetros das conexões clientes e servidor; 181. Deve ser capaz de realizar DHCP *relay*; 182. Deve possuir relatórios das aplicações, com pelos menos os seguintes gráficos: 1. Tempo de resposta da aplicação; 2. Latência; 3. Conexões para conjunto de servidores, servidores individuais; 4. Por URL; 5. A solução deve ter suporte a TLS 1.3.

2	Requisitos do Projeto de Implantação da solução de TI	Os serviços de implantação serão executados pela CONTRATADA e deverão ser estruturados conforme as fases a seguir. I. Fase de abertura a. Validar e Homologar escopo do projeto; b. Validar objetivos e premissas do projeto; c. Validar riscos e restrições do projeto; d. Identificar e validar os requisitos do projeto; e. Efetuar o levantamento de informações sobre o ambiente atual, em complementação ao conjunto de informações apresentado nesta especificação técnica; f. Efetuar o gerenciamento de mudanças, contemplando análise de riscos de implementação do sistema; g. Apresentar o estudo dos riscos envolvidos na migração para o novo sistema a ser implantado. II. Fase de planejamento a. Elaborar plano de projeto; b. Definir as pessoas envolvidas por parte da CONTRATANTE no projeto; c. Reunir as equipes da CONTRATADA e CONTRATANTE; d. 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. III. Fase de execução O serviço de instalação consiste na colocação do(s) equipamento(s) em pleno funcionamento, em conformidade com o disposto neste Estudo, 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 ocaso; 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	Requisitos da Garantia e Manutenção	O suporte, tanto do fabricante quanto do parceiro, deve ser fornecido no modelo 24x7 (24 horas por dia, 7 dias na semana), com garantia e serviços especializados. As funcionalidades da solução (balanceador de carga, global server load balancing, proteção para aplicação, proteção contra ataque DDoS, DNS Application Firewall, inspeção SSL etc) deverão ser licenciadas pelo período de 60 (sessenta) meses. No momento da apresentação das propostas, todos os componentes constantes da Solução deverão possuir EOL (End-of-Life) e EOF (End-of-Support) não definidos ou anunciados. 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.
		Trata-se do serviço de treinamento da solução, na modalidade de fornecimento d e *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:

4	Requisitos de Capacitação	O treinamento deverá oferecer carga horária total de no mínimo 20 (vinte) horas; Serão aceitos preferencialmente treinamentos nas modalidades online ao vivo (EAD), podendo os treinamentos online ao vivo serem gravados, a critério da CONTRATANTE; A CONTRATADA deve prover capacitação técnica em turma com no mínimo 5 (cinco) e no máximo 8 (oito) participantes; Se o treinamento for ofertado na modalidade EAD, deverá respeitar o limite de 4 (quatro) horas por dia; O treinamento deverá cobrir conhecimentos necessários para instalação, administração, configuração, gerência, otimização, resolução de problemas e utilização da solução. As despesas decorrentes do serviço de treinamento (instrutores, confecção do material didático, licenciamento de plataforma de videoconferência etc.) serão de exclusiva responsabilidade da CONTRATADA; O treinamento poderá ser composto de mais de 1 (um) módulo, que deverão ser discriminados na proposta da licitante; 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 cobrem os conhecimentos necessários para instalação, administração, configuração, gerência, otimização, resolução de problemas e utilização da solução; 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; 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; 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; O treinamento deverá ser ministrado por profissionais certificados pelo fabricante, cuja comprovação deverá ser encaminhada na assinatura do Contrato; 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; O treinamento deve ser ministrado em português do Brasil. Caso não exista material oficial do produto em língua portuguesa, será aceito material em inglês; O treinamento deverá oferecer acesso a laboratório prático virtual, fornecido pela contratada, para configuração e execução de exercícios práticos; 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; 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; A ausência do servidor ao treinamento é de responsabilidade do Tribunal, cabendo à contratada informar no certificado a carga horária e assiduidade do servidor; A Contratada deverá aplicar o Formulário de Satisfação, conforme modelo de formulário constante no Anexo III deste Termo de Referência: 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; 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; Caso o resultado da Avaliação de Instrutor seja considerado “não proveitoso”, o treinamento fornecido será considerado não aceito; 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; Na hipótese de o resultado do segundo treinamento ser “não proveitoso”, o objeto será considerado não aceito, aplicando-se as sanções previstas contratualmente
5	Requisitos de Experiência Profissional da Equipe Técnica	A implantação deve ser realizada por profissionais certificados, que possuam certificação do fabricante da solução adquirida ou pelo próprio fabricante, que lhes confiram as competências necessárias para a realização dos respectivos serviços. Para esta solução é necessária a capacitação do corpo técnico e implementação com acompanhamento de um profissional especializado na solução e/ou pelo próprio fabricante, por se tratar de uma solução complexa. A proponente deverá possuir pelo menos 1 (um) profissional capacitado com certificação, e deverá apresentar certificado técnico da solução durante a fase de habilitação. Os profissionais que inicialmente manterão relacionamento direto com o CONTRATANTE deverão ser apresentados após assinatura do CONTRATO na REUNIÃO INICIAL, ocasião em que deverão ser entregues as comprovações dos perfis exigidos. A apresentação de novos profissionais durante a execução do CONTRATO, incluindo a entrega das comprovações dos perfis à equipe de fiscalização do CONTRATO, deverá ser feita previamente ao início da atuação destes.
6	Requisitos de Formação da Equipe Técnica	Não se aplica
7	Requisitos da Metodologia de trabalho	Não se aplica
8	Requisitos de Segurança sob o ponto de vista Técnico	Não se aplica

5.4 – Outros requisitos

ID	TIPO	REQUISITO
1	Não se aplica	

6. IDENTIFICAÇÃO DAS SOLUÇÕES DISPONÍVEIS

	NOME DA SOLUÇÃO:	*Web Application Firewall* - WAF físico baseado em Solução de Mercado

SOLUÇÃO 1	**DESCRIÇÃO:**	Alternativa em que seria adquirido solução WAF do tipo *appliance* físico através de procedimento licitatório próprio. Dentre as possibilidades, há aquela da adesão à ARP do TRE-PA para aquisição de *appliance* físico. Em relação à essa possibilidade, os valores praticados na ARP ficaram muito acima da expectativa do TRE-PI motivo que nos levaram a optar pela versão virtual da solução, conforme Ofício STI 9 (SEI 1540164). Infelizmente, por equívoco, o TRE-PA acabou por excluir o TRE-PI da lista de Regionais interessados em participar da aquisição. Nessa Ata, a unidade do *appliance* físico ficou cotado a R$ 826.398,00 (oitocentos e vinte e seis mil trezentos e noventa e oito reais). Considerando toda a solução (hardware e serviços), a solução tem custo de **R$ 1.756.773,00** (um milhão, setecentos e cinquenta e seis mil setecentos e setenta e três reais). Como o TRE-PI recebeu propostas para *appliances* físicos com custo/benefício mais interessante que aderir à ARP do TRE-PA, a adesão à referida Ata será considerada como alternativa própria e o custo com a solução do TRE-PA não será considerado para a formação do Preço Médio desta solução. • ARP TRE-PA 90/2022 R$ 1.756.773,00 (um milhão, setecentos e cinquenta e seis mil setecentos e setenta e três reais) • PROPOSTA G3 Solutions (SEI nº 1729589) R$ 887.707,67 (oitocentos e oitenta e sete mil setecentos e sete reais e sessenta e sete centavos) • PROPOSTA ClearIT (SEI nº 1730255) R$ 982.760,00 (novecentos e oitenta e dois mil setecentos e sessenta reais) • PROPOSTA IPQ (SEI nº 1736941) R$ 1.417.200,00 (um milhão, quatrocentos e dezessete mil e duzentos reais) • PROPOSTA Logicalis (SEI nº 1739362) R$ 3.274.475,04 (três milhões, duzentos e setenta e quatro mil quatrocentos e setenta e cinco reais e quatro centavos) Devido o alto custo, a proposta da Logicalis não entrará na Formação do Preço Médio. **Preço Médio: R$ 1.261.110,17** (um milhão, duzentos e sessenta e um mil cento e dez reais e dezessete centavos)
	FORNECEDOR(ES):	NTSEC Soluções em Teleinformática LTDA G3 Solutions ClearIT IPQ
	ENTIDADE:	Não se aplica
	VALOR:	R$ 1.261.110,17
	NOME DA SOLUÇÃO:	*Web Application Firewall* - WAF baseado em Software Livre

SOLUÇÃO 2	**DESCRIÇÃO:**	Alternativa em que seria utilizada solução WAF em Software Livre e/ou *Open Source*. Dentre eles, o **ModSecurity** (https://www.modsecurity.org/) da **TrustWave**, que é um dos firewalls de aplicativos da Web mais populares e suporta Apache HTTP, Microsoft IIS e Nginx. O ModSecurity possui uma linguagem de programação robusta baseada em eventos que fornece proteção contra uma série de ataques contra aplicativos da Web e atua principalmente no monitoramento do protocolo HTTP, realizando registro e análise em tempo real. Entretanto, a TrustWave anunciou o fim da vida útil (EOL) do suporte para o ModSecurity a partir de 1º de julho de 2024, informando ainda que a manutenção do código ModSecurity seria entregue de volta à comunidade de código aberto. Outras alternativas são o **Ironbee** e **Zorp**, entretanto as soluções propostas, baseadas em software livre e *open source*, são bastante limitadas se comparadas com os recursos disponíveis em soluções comerciais. Adicionalmente, a solução de segurança WAF requer outros serviços, como treinamentos, suporte especializado para implantação e operação. Além disso, apesar da possibilidade da composição da solução ser factível para Software Livre, as tarefas para integração, implantação e manutenção da solução sobre a equipe de Segurança demandariam elevado tempo até que seja alcançado um nível de proteção minimamente adequado, sendo inclusive inevitável a necessidade de integração de diferentes softwares e soluções, na maioria das vezes, sem a possibilidade de suporte especializado externo. Por contar com uma equipe técnica reduzida para a administração da segurança da informação, o tribunal não teria como solucionar problemas técnicos que poderiam surgir e, sem o suporte técnico especializado de empresas, não teria nem como realizar a contratação desses serviços. Neste cenário, a solução poderia tornar-se limitada ou insuficiente para resolução de ataques emergentes e, em eventual incidente, a correlação e análise detalhada das informações contidas nos softwares de diferentes fontes poderia levar horas ou dias, comprometendo a investigação dos eventos, a preservação de evidências e a disponibilidade e segurança da rede. Portanto, manter e gerenciar uma solução WAF totalmente baseada em softwares livres, para o caso em tela, acarreta custo operacional elevado, bem como alto custo de manutenção do ambiente de missão crítica. Dificulta, ainda, o estabelecimento de processos de gestão da segurança da informação, inviabilizando a especialização da equipe para operação dos sistemas e suas funcionalidades, visto que serão necessários estudos internos e diversos treinamentos para softwares distintos que nem sempre irão garantir sua interoperabilidade.
	FORNECEDOR(ES):	Inviável
	ENTIDADE:	Inviável
	VALOR:	Inviável
SOLUÇÃO 3	**NOME DA SOLUÇÃO:**	Adesão à ARP do TRE-PA
	DESCRIÇÃO:	Alternativa que considera a aquisição de equipamentos do tipo *appliance* físico através da Ata de Registro de Preços nº 91/2022 do TRE-PA. Como dito anteriormente, o TRE-PI informou através do Ofício 9 (SEI nº 1540164) o interesse em ser partícipe do procedimento licitatório liderado pelo TRE-PA, indicando a aquisição de 02 unidades de *appliances* virtuais, uma vez que o preço previsto para este equipamento era menor. No entanto, por equívoco da equipe do TRE-PA, este Tribunal não foi incluído na referida ARP. Caso fossem adquiridos os dois *appliances* físicos através dessa ARP, seriam necessários **R$ 1.652.796,00** (um milhão, seiscentos e cinquenta e dois mil setecentos e noventa e seis reais). Adicionalmente, seriam necessários **R$ 41.036,00** (quarenta e um mil trinta e seis reais) para Instalação e repasse de conhecimento na modalidade *hands-on*; **R$ 23.691,00** (vinte e três mil seiscentos e noventa e um reais) para serviço de operação assistida; e **R$ 39.250,00** (trinta e nove mil duzentos e cinquenta reais) para a participação de dois alunos em treinamento especializado. Totalizando, o Tribunal necessitaria arcar com, no mínimo, **R$ 1.756.773,00** (um milhão, setecentos e cinquenta e seis mil setecentos e setenta e três reais) para adquirir 02 (dois) *appliances* físicos e realizar o treinamento de 02 servidores.
	FORNECEDOR(ES):	NTSEC SOLUCOES EM TELEINFORMATICA LTDA
	ENTIDADE:	TRE-PA
	VALOR:	R$ 1.756.773,00
	NOME DA SOLUÇÃO:	*Web Application Firewall* - WAF virtual baseado em Solução de Mercado

SOLUÇÃO 4	**DESCRIÇÃO:**	Alternativa em que seria adquirido solução WAF do tipo *appliance* virtual Para essa aquisição, poder-se-ia aderir à ARP do TRE-PA ou realizar um procedimento próprio. Inicialmente, o TRE-PI optou por adquirir solução virtual uma vez que os valores previstos no procedimento licitatório do TRE-PA para a solução física eram bem superiores à disponibilidade orçamentária. • ARP TRE-PA 90/2022 (SEI nº 1729587) R$ 1.103.123 (um milhão, cento e três mil cento e vinte e três reais) • Contrato TRE-BA 14/2022 R$ 996.000,00 • PROPOSTA SERVIX (SEI nº) R$ 748.452,00 (setecentos e quarenta e oito mil quatrocentos e cinquenta e dois reais) **Preço Médio: R$ 949.191,67** (novecentos e quarenta e nove mil cento e noventa e um reais e sessenta e sete centavos)
	FORNECEDOR(ES):	NTSEC Soluções em Teleinformática LTDA PTLS Serviços de Tecnologia e Assessoria Técnica LTDA SERVIX
	ENTIDADE:	TRE-PA, TRE-BA
	VALOR:	R$ 949.191,67

7. DETALHAMENTO DAS SOLUÇÕES E ALTERNATIVAS EXISTENTES

REQUISITO	ID DA SOLUÇÃO	SIM	NÃO	NÃO SE APLICA
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública Federal?	1	x		
	2		x	
	3	x		
	4	x		
A Solução encontra-se implantada em outro órgão ou entidade da Justiça Eleitoral?	1	x		
	2		x	
	3	x		
	4	x		
A Solução está disponível no Portal do Software Público Brasileiro?	1		x	
	2		x	
	3		x	
	4		x	
A Solução é um software livre ou software público?	1		x	
	2	x		
	3		x	
	4		x	
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões e-PING, e-MAG?	1		x	
	2		x	
	3		x	
	4		x	
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	1		x	
	2		x	
	3		x	
	4		x	
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Judiciário – MoReq-Jus?	1		x	
	2		x	
	3		x	
	4		x	

8. ANÁLISE E COMPARAÇÃO DOS CUSTOS TOTAIS DA DEMANDA

A **Solução 1**, que trata da aquisição de *Web Application Firewall* - WAF físico baseado em Solução de Mercado, tem custo de **R$ 1.261.110,17** (um milhão, duzentos e sessenta e um mil cento e dez reais e dezessete centavos). No cálculo do preço médio dessa solução não foi considerada a proposta da empresa Logicalis pois seu preço é muito divergente dos demais. opção pela ARP do TRE-PA uma vez que o custo para aquisição de solução semelhante utilizando a referida ARP é muito superior ao Preço Médio aqui calculado.

A **Solução 2**, que trata da aquisição de *Web Application Firewall* - WAF baseado em Software Livre não possui custo inicial. No entanto, esse tipo de contratação não possuiria suporte de empresa especializada, dependendo principalmente da ajuda da comunidade. O risco de depender da comunidade para resolução de problemas é muito alto para ser assumido pelo Tribunal, inviabilizando essa solução.

A **Solução 3**, que trata da adesão à ARP do TRE-PA, tem custo de **R$ 1.756.773,00** (um milhão, setecentos e cinquenta e seis mil setecentos e setenta e três reais) para aquisição de solução com *appliances* físicos. Pode-se verificar que o custo desta solução é bastante superior ao custo da Solução 1, sendo que as duas tem por objetivo a aquisição de solução similares.

Como pode-se verificar da Ata de Realização do Pregão Eletrônico TRE-PA 46/2022 (SEI nº 1725565), apenas 3 empresas participaram da licitação, sendo que duas delas ofertando a mesma solução (F5). Sabendo disso, realizamos pequenas modificações que, a nosso ver, incentivarão a concorrência, atraindo mais empresas interessadas e diminuindo o custo da aquisição.

A **Solução 4**, que trata da aquisição de **Web Application Firewall** - WAF virtual baseado em Solução de Mercado, tem custo de **R$ 949.191,67** (novecentos e quarenta e nove mil cento e noventa e um reais e sessenta e sete centavos). Inicialmente, o TRE-PI decidiu participar da ARP do TRE-PA optando por uma solução virtual devido ao elevado custo de uma solução física. Algo que se deve ter em mente para esta solução, é que ela estará inserida no ambiente de virtualização do Tribunal, consumindo recursos que deveriam estar dedicados aos serviços internos disponibilizados aos usuários. Outro fato importante, é que utilizará hardware genérico (chassi blade/hipercovergência). Isso também impacta o desempenho na execução de algumas funções (decriptografia SSL, por exemplo), que é muito mais performática em hardware próprio para isso.

Conforme verifica-se na Planilha de Formação de Preço Médio (SEI nº 1739592), a solução baseada em *appliance* virtual tem preço menor que a solução baseada em *appliance* físico. No entanto, algumas observações devem ser feitas. A solução física ficará totalmente apartada do ambiente de virtualização, criando um perímetro de segurança sobre a infraestrutura tecnológica do Tribunal. Além disso, algumas funcionalidades requeridas tem melhor desempenho quando executadas sobre hardware próprio e especializado, não havendo a necessidade de disputar recursos com outros serviços. Além disso, por estar fora da infraestrutura de virtualização, o impacto sobre os serviços internos é menor pois necessitará de menos intervenções.

Podemos verificar, também, a existência de propostas abaixo do preço médio calculado. A exclusão do custo da solução prevista na ARP do TRE-PA no cálculo do preço médio leva o preço médio para R$ 1.095.889,22 (um milhão, noventa e cinco mil oitocentos e oitenta e nove reais e vinte e dois centavos), apenas R$ 146.697,55 acima do preço médio de uma solução virtual. Se considerarmos no cálculo do preço médio apenas as duas menores propostas, o valor da solução física ficará menor que o custo da solução virtual.

Acreditamos que durante o pregão eletrônico, o custo da solução deverá cair ficando bem abaixo do que foi calculado neste ETP.

9. SOLUÇÃO ESCOLHIDA

9.1 – Identificação

NOME:	*Web Application Firewall* - WAF fisico baseado em Solução de Mercado		
JUSTIFICATIVA:	Esta solução atende a todos os requisitos levantados além de ter um melhor custo/benefício que o conseguido pelo TRE-PA		
DESCRIÇÃO:	Aquisição de solução de cluster de *appliance* físico de WAF com garantia e suporte por 60 (sessenta) meses.		
BENS E SERVIÇOS	**ID**	**BEM / SERVIÇO**	**VALOR ESTIMADO**
	1	Solução de *Web Application Firewall* (WAF), do tipo *appliance* físico com garantia de 60 meses	R$ 1.140.396,75
	2	Serviço de Instalação e repasse de conhecimento Hands-on	R$ 46.988,17
	3	Treinamento especializado	R$ 45.362,50
	4	Banco de horas para suporte e consultoria	R$ 28.362,75

9.2 – Alinhamento com as necessidades de negócio

ID	FUNÇÃO	NECESSIDADE DO NEGÓCIO
1	Inspeção SSL	Proteção de servidores que hospedam aplicações WEB
2	Decriptografia do tráfego SSL em hardware dedicado	Proteção de servidores que hospedam aplicações WEB
3	Balanceamento de carga por: hash, persistent hash, least connections, least connections per service, round-robin, response time e bandwitch	Balanceamento de carga
4	Proteção de aplicações WEB contra ameaças registradas no OWASP Top Ten Vulnerabilities	Monitoramento e detecção de ataques
5	Proteção contra ataques em camada de aplicação WEB, como: XSS, SQL Injections, OS command injections, Sensitive information leakage, CSRF, Application Dos, etc	Redução da superfície de ataques cibernéticos da Justiça Eleitoral

9.3 – Benefícios esperados

ID	TIPO	BENEFÍCIOS
1	Infraestrutura	Modernização da infraestrutura de Segurança da Informação
2	Segurança da Informação	Aumentar a disponibilidade, integridade e confiabilidade dos sistemas do Tribunal
3	Compliance	Conformidade com padrões, regulamentos internos e externos

9.4 – Justificativa de não-conformidade

ID	SOLUÇÃO	JUSTIFICATIVA
1	Web Application Firewall - WAF baseado em Software Livre	A solução baseada em software livre não atende todas as especificações, havendo a necessidade de agregar várias soluções distintas para que trabalhem conjuntamente (balanceamento de carga, waf, etc), aumentando a complexidade da infraestrutura. O suporte teria que ser prestado pela comunidade, podendo causar eventuais indisponibilidades. Não há garantia de atualizações quando detectadas novas ameaças.
2	Adesão à ARP do TRE-PA	Apesar de inicialmente termos optado por participar da ARP liderada pelo TRE-PA, este Regional não incluiu o nome do TRE-PI o que nos obrigou a realizar procedimento próprio. Por conta do alto valor do equipamento do tipo *appliance* físico e do recebimento de propostas com valor mais atrativo, decidimos não aderir à Ata e realizar uma própria.
3	*Web Application Firewall* - WAF virtual em Solução de Mercado	Apesar de atender as especificações, a solução virtual necessitaria ser implantada na infraestrutura de virtualização do Tribunal, consumindo recursos disponíveis para os serviços internos. Alguns recursos da solução (decriptografia SSL, etc), tem um melhor desempenho em hardware especializado para aquela determinada finalidade que rodando sobre hardware genérico. Qualquer comprometimento do *appliance* virtual (má configuração, defeito, *zero day*, etc), poderia facilitar o acesso não autorizado à rede do TRE-PI uma vez que o invasor já estaria dentro da infraestrutura. Adicionalmente, os custos com a aquisição de um *appliance* físico através de procedimento próprio mostraram-se mais atraentes.

10. AVALIAÇÃO DAS NECESSIDADES DE ADEQUAÇÃO PARA EXECUÇÃO CONTRATUAL

ID	TIPO DE NECESSIDADE	SIM	NÃO	DESCRIÇÃO
1	Infraestrutura Tecnológica		x	Necessidade de utilização da rede lógica corporativa do Tribunal Necessidade de instalação no Datacenter do Tribunal
2	Infraestrutura Elétrica		x	Solução será instalada no Datacenter e utilizará alimentação proveniente de suas UPS
3	Logística de implantação	x		Após a entrega dos equipamentos pela CONTRATADA, recebimento e aceite pela fiscalização do Contrato, estes deverão ser configurados e instalados, também pela CONTRATADA, com supervisão da equipe técnica do CONTRATANTE. 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. 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.
4	Espaço Físico	x		Será disponibilizado espaço físico no rack do Datacenter para a instalação dos equipamentos da solução a ser contratada
5	Mobiliário		x	Não se aplica
6	Impacto ambiental		x	Não se aplica

11. RECURSOS NECESSÁRIOS À CONTINUIDADE DO NEGÓCIO DURANTE E APÓS A EXECUÇÃO DO CONTRATO

DESCRIÇÃO DOS RECURSOS NECESSÁRIOS PARA SUPORTAR A CONTRATAÇÃO DA SOLUÇÃO		
11.1. Recursos Materiais		
Item	**Descrição**	
1	Não se aplica	
11.2. Recursos Humanos		
Item	**Função**	**Formação**
1	Técnico	Conhecimento de redes Conhecimento em segurança da informação Capacitação na solução adquirida

12. ESTRATÉGICA DE CONTINUIDADE CONTRATUAL

IDENTIFICAÇÃO DE EVENTOS QUE POSSAM CAUSAR INTERRUPÇÃO CONTRATUAL			
Evento	**Descrição**	**Ação de Contingência**	**Responsável**
1	Defeito em equipamento	Implementação da solução em cluster	Equipe de planejamento
2	Fim do período do suporte e garantia técnica	Deliberação acerca da necessidade de nova contratação da garantia técnica da solução para upgrade e/ou renovação das licenças e suporte da solução	STI
3	Fim do banco de horas para suporte e consultoria	Renovação desse item contratado por mais 12 (doze) meses, com utilização sob demanda	SELIC

13. AÇÕES PARA TRANSIÇÃO E ENCERRAMENTO CONTRATUAL

Item	Ação	Responsável	Data Início	Data Fim
1	Decisão por nova aquisição ou contratação de extensão de suporte	STI	07/01/2028	30/05/2028

14. ESTRATÉGIA DE INDEPENDÊNCIA

14.1. Transferência de Conhecimento Tecnológico		
Item	**Informações que deverão ser transmitidas pela Contratada**	**Forma de transferência do Conhecimento**
1	Implantação e repasse de conhecimento Hands-on	Repasse hands-on com carga horária de, no mínimo, 6 horas para o repasse de conhecimento Repasse deverá cobrir conhecimentos para administração, configuração, otimização, resolução de problemas e utilização da solução.
2	Treinamento especializado	Fornecimento de voucher para treinamento cobrindo 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	Banco de Horas	Estabelecimento de banco de horas de, no mínimo, 80 horas para suporte e consultoria a ser utilizado sob demanda ao longo de 12 (doze) meses.
14.2. Direitos de Propriedade Intelectual e Autorais		
Item	**Cláusulas segundo a lei Nº 9.610, de 19 de fevereiro de 1998.**	
1	O instrumento contratual deve estabelecer que os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, os modelos de dados e as bases de dados, pertençam à Administração;	
2	A Contratada deverá ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, os modelos de dados e as bases de dados à Administração.	

15. ANÁLISE DE RISCOS

15.1 – Riscos do processo de contratação (identificar os riscos que podem comprometer o processo de contratação, resultando em atrasos ou em comprometimento do processo de contratação – IN04, art. 16, I)

RISCO 1					**PROBABILIDADE**	
Não aprovação dos documentos do Planejamento da Contratação /documentos incompletos					( ) 1-Baixo (x) 2-Médio ( ) 3-Alto ( ) 4-Muito alto	
ID	**EFEITO**	**IMPACTO**	**AÇÃO DE RESPOSTA AO RISCO**	**TIPO DE AÇÃO**	**RESPONSÁVEL**	**ÁREA**
1	Atraso no processo de contratação	( ) 1-Baixo (x) 2-Médio ( ) 3-Alto ( ) 4-Muito alto	Adotar procedimentos para que a área administrativa acompanhe a elaboração, análise crítica e revisão dos documentos, evitando envios e devoluções do processo	(x) 1-Mitigação ( ) 2-Contingência	Equipe de Planejamento	STI / SAOF
2	Atraso no processo de contratação	( ) 1-Baixo (x) 2-Médio ( ) 3-Alto ( ) 4-Muito alto	Reuniões com superiores para sensibilização, priorização da tramitação processual e aprovação dos documentos.	(x) 1-Mitigação ( ) 2-Contingência	Equipe de Planejamento	STI / SAOF

RISCO 2					PROBABILIDADE	
Insuficiência de recursos orçamentários/financeiros para aquisição					(x) 1-Baixo ( ) 2-Médio ( ) 3-Alto ( ) 4-Muito alto	
ID	**EFEITO**	**IMPACTO**	**AÇÃO DE RESPOSTA AO RISCO**	**TIPO DE AÇÃO**	**RESPONSÁVEL**	**ÁREA**
1	Atraso no processo de contratação	( ) 1-Baixo (x) 2-Médio ( ) 3-Alto ( ) 4-Muito alto	Encontrar a maneira mais vantajosa economicamente para realizar a contratação	(x) 1-Mitigação ( ) 2-Contingência	Equipe de Planejamento	STI / SAOF
2	Atraso no processo de contratação	( ) 1-Baixo (x) 2-Médio ( ) 3-Alto ( ) 4-Muito alto	Utilização de recursos destinados a outras aquisições para contemplar esta necessidade	( ) 1-Mitigação (x) 2-Contingência	Equipe de Planejamento	STI / SAOF
3	Atraso no processo de contratação	( ) 1-Baixo (x) 2-Médio ( ) 3-Alto ( ) 4-Muito alto	Solicitar orçamento	(x) 1-Mitigação ( ) 2-Contingência	Equipe de Planejamento	STI / SAOF
4	Atraso no processo de contratação	( ) 1-Baixo (x) 2-Médio ( ) 3-Alto ( ) 4-Muito alto	Remanejar verbas de outros projetos previstos no plano de contratações mas que não serão executados por razões diversas	( ) 1-Mitigação (x) 2-Contingência	SAOF	SAOF

RISCO 3					PROBABILIDADE	
Atraso na Aquisição					( ) 1-Baixo (X) 2-Médio ( ) 3-Alto ( ) 4-Muito alto	
ID	**EFEITO**	**IMPACTO**	**AÇÃO DE RESPOSTA AO RISCO**	**TIPO DE AÇÃO**	**RESPONSÁVEL**	**ÁREA**
1	Aumento do risco em caso de inoperância Paralisação do ambiente dos sistemas e dos serviços associados.	( ) 1-Baixo ( ) 2-Médio (x) 3-Alto ( ) 4-Muito alto	Solicitação de aceleração de trâmites internos	(x) 1-Mitigação ( ) 2-Contingência	Equipe de Planejamento	STI / SAOF

RISCO 4					PROBABILIDADE	
Descumprimento de cláusulas contratuais relativas ao fornecimento da solução					(X) 1-Baixo ( ) 2-Médio ( ) 3-Alto ( ) 4-Muito alto	
ID	**EFEITO**	**IMPACTO**	**AÇÃO DE RESPOSTA AO RISCO**	**TIPO DE AÇÃO**	**RESPONSÁVEL**	**ÁREA**
1	Atraso na entrega do objeto	( ) 1-Baixo (x) 2-Médio ( ) 3-Alto ( ) 4-Muito alto	Definição de níveis de serviços adequados, como prazo de entrega exequível.	(x) 1-Mitigação ( ) 2-Contingência	Equipe de Planejamento	STI / SAOF
2	Não entrega do objeto	( ) 1-Baixo (x) 2-Médio ( ) 3-Alto ( ) 4-Muito alto	Definição de cláusulas relativas ao descumprimento de exigências do instrumento convocatório com aplicação multa moratórias.	(x) 1-Mitigação ( ) 2-Contingência	Equipe de Planejamento	STI / SAOF
3	Entrega do material/serviço em divergência ao exigido no Edital.	( ) 1-Baixo (x) 2-Médio ( ) 3-Alto ( ) 4-Muito alto	Acompanhamento e verificação de qualidade do serviço prestado. Incentivo à solução do desvio de qualidade por meio de aplicação de glosas e, caso haja prejuízo maior previsto nos níveis de serviço, aplicação das sanções cabíveis, de forma a coibir a incidência (ou reincidência).	(x) 1-Mitigação ( ) 2-Contingência	Equipe de Fiscalização	STI / SAOF

4	Fornecimento incompleto dos serviços de infraestrutura de TI.	( ) 1-Baixo (x) 2-Médio ( ) 3-Alto ( ) 4-Muito alto	Acompanhar a execução do contrato, no que tange a instalação e configuração os equipamentos fornecidos Dividir o fornecimento em etapas e incluir no instrumento convocatório condições que obriguem a Contratada fornecer documentação ou roteiro relativo a configuração do(s) equipamento(s) fornecido(s)ou serviços prestados. Multa moratória pela inexecução parcial	(x) 1-Mitigação ( ) 2-Contingência	Equipe de Fiscalização	STI / SAOF

RISCO 5					**PROBABILIDADE**	
Término do contrato de garantia					( ) 1-Baixo (x) 2-Médio ( ) 3-Alto ( ) 4-Muito alto	
ID	**EFEITO**	**IMPACTO**	**AÇÃO DE RESPOSTA AO RISCO**	**TIPO DE AÇÃO**	**RESPONSÁVEL**	**ÁREA**
1	Ameaça à continuidade da proteção de dados dos serviços essenciais.	( ) 1-Baixo ( ) 2-Médio (x) 3-Alto ( ) 4-Muito alto	Providenciar nova contratação de extensão de garantia	( ) 1-Mitigação (x) 2-Contingência	Equipe de Fiscalização	STI / SAOF
2	Comprometimento do funcionamento da solução	( ) 1-Baixo ( ) 2-Médio (x) 3-Alto ( ) 4-Muito alto	Primar pela execução das atividades críticas, que comprometam a disponibilidade do ambiente tecnológico.	( ) 1-Mitigação (x) 2-Contingência	STI	STI / SAOF

15.2 – Riscos da solução de TI escolhida (identificar os riscos que podem fazer com que, após o serviço ter sido contratado, o mesmo não atenda às necessidades do negócio especificadas – IN04, art. 16, II)

RISCO 1					**PROBABILIDADE**	
Serviços de TI não especificados adequadamente					( ) 1-Baixo (x) 2-Médio ( ) 3-Alto ( ) 4-Muito alto	
ID	**DANO**	**IMPACTO**	**AÇÃO DE RESPOSTA AO RISCO**	**TIPO DE AÇÃO**	**RESPONSÁVEL**	**ÁREA**
1	Deixar de mencionar alguma funcionalidade necessária ao Tribunal	( ) 1-Baixo ( ) 2-Médio (x) 3-Alto ( ) 4-Muito alto	Realizar vasta pesquisa de contratos realizados por outros órgãos	(x) 1-Mitigação ( ) 2-Contingência	Equipe de Planejamento	STI / SAOF

16. ESTRATÉGIA PARA CONTRATAÇÃO

16.1. SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (Res. CNJ 182/2013, art. 16)

16.1.1 – DEFINIÇÃO (NATUREZA DO OBJETO) DA SOLUÇÃO (critérios que serão usados para definir o tipo de contratação, modalidade de licitação, etc: inovação tecnológica ou serviço/bem comum; necessidade pontual ou contínua- Res. CNJ 182/2013, art. 16, IV)	
Critério	**Atendimento da Solução**
É possível especificar o serviço usando parâmetros usuais de mercado?	Sim
É possível medir o desempenho da qualidade usando parâmetros usuais de mercado?	Sim
O objeto da contratação se estende necessariamente por mais de um ano?	Sim. Os serviços de garantia e suporte técnicos das soluções de backup se estendem por mais de um ano, pois são necessários para a realização e armazenamento das cópias de segurança de todos os dados dos sistemas informatizados do Tribunal, o que caracteriza a sua natureza continuada.

O objeto da contratação é essencial para o negócio?	Sim. A disponibilização de serviços via WEB é fundamental para a implementação do Plano de Transformação Digital. Nesse sentido, se faz necessário que essa disponibilização ocorra com níveis mínimos de segurança e disponibilidade

16.1.2 – PARCELAMENTO E ADJUDICAÇÃO DA CONTRATAÇÃO (justificar se é técnica e economicamente viável dividir a solução a ser contratada. Informar se o objeto pode ou não ser dividido em itens ou até mesmo em grupos. Em caso de divisão, verificar se há prejuízo nos resultados finais a serem obtidos. De acordo com o parcelamento do objeto, informar se a adjudicação pode ou não ser realizada para mais de um fornecedor. Justificar a escolha. Esse item não se aplica aos casos de Dispensa ou Inexigibilidade - (Res. CNJ 182/2013, art. 16, II e III)

A aquisição se dará por adjudicação global não sendo possível seu parcelamento. Devido necessidade de redundância, alta disponibilidade e ponto de gerenciamento único, não é possível a aquisição de equipamentos de marcar/modelos distintos.

16.2. RESPONSABILIDADES DA CONTRATANTE E DA CONTRATADA

16.2.1 – DEVERES E RESPONSABILIDADES DA CONTRATANTE (deveres e responsabilidades da contratante que comporão o contrato)

ID	Dever / Responsabilidade
1	Receber o objeto no prazo e condições estabelecidas no Edital e seus anexos. 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. 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. Abrir e acompanhar os chamados técnicos à contratada, elaborando relatórios mensais, constando as conformidades e desconformidades dos serviços prestados. Comunicar à Contratada, por escrito, sobre imperfeições, falhas ou irregularidades verificadas no objeto fornecido, para que seja substituído, reparado ou corrigido. Acompanhar e fiscalizar o cumprimento das obrigações da Contratada, através de comissão/servidor especialmente designado. Atestar a(s) notas fiscal(ais) apresentada(s) pela CONTRATADA após o recebimento definitivo dos equipamentos, conforme especificações descritas neste Termo de Referência. Efetuar o pagamento à Contratada no valor correspondente ao fornecimento do objeto, no prazo e forma estabelecidos no Edital e seus anexos. Prestar informações e esclarecimentos que venham a ser solicitados pela CONTRATADA, necessários à execução do contratado.

16.2.2 – DEVERES E RESPONSABILIDADES DA(S) CONTRATADA(S) (deveres e responsabilidades da(s) contratada(s) que comporão o contrato. A(s) contratada(s) não poderá(ão) se eximir dessas responsabilidades, mesmo havendo subcontratação - (IN04, art. 15, II)

ID	Dever / Responsabilidade

1	A CONTRATADA obriga-se a fornecer o material obedecendo rigorosamente às especificações discriminadas neste Termo de Referência. Manter, durante o fornecimento, todas as condições de habilitação e qualificação exigidas neste Termo de Referência. Não transferir a outrem, no todo ou em parte, o objeto do contrato a ser firmado. 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 Atender aos chamados técnicos no prazo estipulado pela contratante 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) Substituir, reparar ou corrigir, às suas expensas, no prazo fixado neste Termo de Referência (item 9.2.3), o objeto com avarias ou defeitos. Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação. Responsabilizar-se integralmente pelo fiel cumprimento do objeto contratado, prestando todos os esclarecimentos que forem solicitados pela CONTRATANTE, cujas reclamações se obriga a atender. Apresentar o Termo de Confidencialidade e Sigilo (Anexo I) dos envolvidos na implantação da solução, migração de dados e operação assistida. Prover assistência técnica no **território** brasileiro. **Dar garantia não inferior a 60 meses, a contar da data de emissão do Termo de Recebimento Definitivo;**

16.3 INDICAÇÃO DOS TERMOS CONTRATUAIS (IN04, art. 15, III)

16.3.1 – PROCEDIMENTOS E CRITÉRIOS DE ACEITAÇÃO (IN04, art. 15, III, a)

ID	**Etapa / Fase / Item** (em qual etapa, fase ou item do projeto será aplicada a mensuração)	**Indicador** (qual será o indicador mensurado. Qual será a unidade de medida a ser avaliada)	**Valor Mínimo Aceitável** (valor mínimo aceitável daquele item de mensuração)
1	Aceitação da proposta	Configurações dos equipamentos/serviços ofertados	Especificação mínima exigida em edital
2	Implantação da solução	Carga horária do treinamento	Carga horária mínima de 06 horas
3	Recebimento definitivo	Adequação dos equipamentos/serviços	Especificação mínima exigida em edital
4	Recebimento definitivo	Garantia dos equipamentos	Garantia de 60 (sessenta) meses
5	Recebimento definitivo	Suporte dos softwares/licenças entregues	Suporte de 60 (sessenta) meses

16.3.2 – FORMA DE PAGAMENTO (modo ou percentual que será pago por cada entrega em função do resultado a ser obtido -IN04, art. 15, III, e)

O pagamento será efetuado por meio de depósito bancário em conta corrente, até o 10º (décimo) dia útil a partir da emissão do Termo de Aceite Definitivo, devidamente certificada pela equipe de contratação e processada na forma da legislação vigente.

O pagamento relativo ao banco de horas para suporte/consultoria será realizado até o 10º (décimo) dia útil a partir da entrega da fatura de serviço, considerando-se os chamados abertos e encerrados dentro do mês de referência.

16.3.3 – CRONOGRAMA DE EXECUÇÃO FÍSICO-FINANCEIRA (IN04, art. 15, III, f)

ID	**Entrega** (listagem do item ou serviço a ser entregue. Esta entrega pode ser parcelada ou integral)	**Data de Entrega**	**Percentual a ser Pago**
1	*Web Application Firewall*	Até 90 (noventa) dias após recebimento da ordem fornecimento	0%
2	Serviço de Instalação e repasse de conhecimento *Hands-on*	Até 30 (trinta) dias após confirmação do recebimento da ordem de serviço	100% sobre o valor do Item 1 100% sobre o valor do item 2
3	Treinamento especializado	A ser agendado com equipe técnica	100% sobre o valor do item 3
4	Banco de horas para suporte e consultoria	Sob demanda	Até 100% sobre o valor do item 4
Total:		R$ 1.261.110,17	100%

16.3.4 – MECANISMOS FORMAIS DE COMUNICAÇÃO (IN04, art. 15, III, g)

Função de Com. 1 (listagem do que deverá ser contemplado neste mecanismo de comunicação):	Assinatura de contrato, emissão de ordem de fornecimento, emissão de notas fiscais.			
Documento (nome do documento a ser entregue)	**Emissor**	**Destinatário**	**Meio** (forma com que o documento deverá ser produzido e entregue)	**Periodicidade** (frequência que os documentos deverão ser emitidos e entregues pela contratada ou pela administração)
Ata de Registro de Preços	Contratante	Contratada	Eletrônico	1 vez
Contrato	Contratante	Contratada	Eletrônico	1 vez
Ordem de Fornecimento	Contratante	Contratada	Eletrônico	1 vez para cada unidade do item 1, considerando a disponibilidade orçamentária.
Nota Fiscal	Contratada	Contratante	Físico / Eletrônico	Uma única vez a cada Ordem de Fornecimento
Nota de Empenho	Contratante	Contratada	Eletrônico	Uma única vez a cada Ordem de Fornecimento
Abertura de chamado	Contratante	Contratada	Eletrônico	Mensalmente, sempre que houver chamado concluído no mês de referêcia

16.3.5 – REGRAS PARA APLICAÇÃO DE MULTAS E SANÇÕES (IN04, art. 15, III, h)		
ID	**Ocorrência** (descrição clara das situações em que se caracterizará a infração a algum termo contratual. Devem ser descritas as não conformidades, ou outras situações ou ocorrências em que serão propostas sanções a serem aplicadas pela Área Administrativa)	**Sanção / Multa** (descrição da sanção/multa a ser aplicada de acordo com cada situação ou ocorrência listada. As multas e sanções devem ser proporcionais ao impacto que a ocorrência provocará no órgão e aos casos de reincidência das ocorrências)
1	• Não assinar o contrato ou Ata de Registro de Preços • Deixar de entregar documentação exigida neste edital; • Apresentar documentação falsa; • Não manter a proposta; • Falhar ou fraudar na execução do contrato; • Comportar-se de modo inidôneo; • Fazer declaração falsa; • Cometer fraude fiscal.	Fundamentado no artigo 7º da Lei 10.520/2002, regulamentado pelo artigo 49 do Decreto n.º 10.024/2019, ficará impedido de licitar e contratar com a União e será descredenciado no SICAF, pelo prazo de até 05 (cinco) anos, garantido o direito à ampla defesa
2	Faltas leves, assim entendidas aquelas que não acarretem prejuízos significativos para a Contratante.	Penalidade de advertência
3	• Atraso no cumprimento das obrigações assumidas contratualmente, que tenha acarretado prejuízos financeiros para o TRE-PI; • Entrega de objeto, em desacordo com a proposta aceita pela Contratante, sem prejuízo das demais sanções.	Suspensão temporária de participação em licitação e impedimento de contratar com o TRE-PI, p**or até 1 (um) ano,** se, por culpa ou dolo, prejudicar ou tentar prejudicar a execução do Contrato

4	• Entrega de objeto falso, seja como amostra ou como bem a ser entregue por ocasião de emissão de ordem de fornecimento, assim entendido, aquele em que houve manipulação para aparentar ser de outra marca/fabricante, ou ter características que originalmente não lhe pertençam, sem prejuízo das demais medidas cabíveis; • Não atendimento à solicitação de troca ou prestação de garantia do objeto, quando solicitado pela Contratante, no prazo fixado no edital • Cometimento de quaisquer outras irregularidades que acarretem prejuízo ao TRE-PI, ensejando a rescisão do Contrato por culpa da CONTRATADA; • Apresentação, ao TRE-PI, de qualquer documento falso ou falsificado, no todo ou em parte, com o objetivo de comprovar, durante a execução do Contrato, a manutenção das condições apresentadas na habilitação	Suspensão temporária de participação em licitação e impedimento de contratar com o TRE-PI, p**or até 2 (dois) anos,** se, por culpa ou dolo, prejudicar ou tentar prejudicar a execução do Contrato
5	Entrega do objeto com atraso	Multa moratória mensurada na forma de tabela a ser prevista no termo de referência, até o limite de 13% (treze por cento), calculada sobre o valor do objeto em atraso
6	Inexecução total do contrato	Multa compensatória de 15% (quinze por cento) sobre o valor do objeto

16.4. CRITÉRIOS TÉCNICOS DE JULGAMENTO DAS PROPOSTAS (IN04, art. 15, VII)

16.4.1 – CRITÉRIOS DE SELEÇÃO			
( ) Licitação (X) Registro de Preço ( ) Dispensa de licitação ( ) Inexigibilidade de licitação			
Modalidade:	Pregão Eletrônico	**Tipo:**	Menor preço global
Justificativa: (obrigatório se for dispensa ou inexigibilidade de licitação)	O objeto da contratação pretendida possui requisitos de desempenho e qualidade objetivamente definidos por meio de especificações usuais de mercado, razão por que se entende adequada a utilização do Pregão Eletrônico. Considerando a incerteza de disponibilidade de recursos orçamentários para a aquisição da totalidade da demanda indicada no presente exercício financeiro, bem como a possível expansão da solução em função do crescimento da demanda, através da adesão de outros Regionais, entende-se necessária a realização de Pregão Eletrônico com Sistema de Registro de Preços, conforme o art. 3º do Decreto Nº 7.892/2013.		

16.5. INDICAÇÃO DA EQUIPE DE GESTÃO DA CONTRATAÇÃO (ou comissão de recebimento de bens) (Res. CNJ 182/2013, art. 16, VIII)

Gestor do Contrato:	Rosemberg Maia Gomes	Telefone:	86 2107-9762
E-mail do Gestor do Contrato:	rosemberg.maia@tre-pi.jus.br	Setor:	CODIN
Fiscal Demandante:	Rosemberg Maia Gomes	Telefone:	86 2107-9762
E-mail do Fiscal Demandante:	rosemberg.maia@tre-pi.jus.br	Setor:	CODIN
Fiscal Técnico:	Carlos Alberto Ribeiro do Nascimento Jr	Telefone:	86 2107-9756
E-mail do Fiscal Técnico:	carlos.nascimento@tre-pi.jus.br	Setor:	SEINF
Fiscal Administrativo:	Vivianne Furtado de Carvalho Silva	Telefone:	86 2107-9858
E-mail do Fiscal Administrativo:	vivianne.silva@tre-pi.jus.br	Setor:	SELIC

17. ASSINATURAS

INTEGRANTE	NOME	ÁREA
Demandante:	Rosemberg Maia Gomes	CODIN
Técnico:	Carlos Alberto Ribeiro do Nascimento Jr.	SEINF
Administrativo:	Vivianne Furtado de Carvalho Silva	SELIC

Teresina, 06 de dezembro de 2022.

Documento assinado eletronicamente por **Carlos Alberto Ribeiro do Nascimento Junior**, **Chefe de Seção**, em 16/12/2022, às 12:16, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Rosemberg Maia Gomes**, **Coordenador de Desenvolvimento e Infraestrutura**, em 16/12/2022, às 12:23, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-pi.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1729580** e o código CRC **82FBE7CA**.