TRIBUNAL REGIONAL ELEITORAL DO PIAUÍ

Termo de Referência Nº 11

1. OBJETO

1.1. Registro de preços para eventual e futura aquisição de **Solução de *Web Application Firewall*** (WAF) e balanceamento de carga, incluindo serviços de implantação, transferência tecnológica (*hands-on*), treinamento especializado, operação assistida e garantia da solução por 60 (sessenta) meses, conforme as especificações e condições estabelecidas neste Termo de Referência.

1.2. Justificativa para o agrupamento de itens.

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

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

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

1.2.4. Isto posto, o agrupamento dos itens visa garantir a compatibilidade técnica e operacional entre os componentes da solução, visto que haverá integração entre software, hardware e repasse tecnológico, a contratação será realizada através de um único grupo.

1.3. O registro de preços terá validade de 12 (doze) meses, a contar da publicação do extrato da respectiva ata.

	ITEM	DESCRIÇÃO	QTDE REGISTRADA
GRUPO ÚNICO	1	Solução de *Web Application Firewall* (WAF), do tipo *appliance* físico com garantia e suporte de 60 meses	2
	2	Serviço de Instalação e repasse de conhecimento Hands-on	1
	3	Treinamento especializado	1
	4	Banco de horas para suporte e consultoria	80hs
	VALOR ESTIMADO DA CONTRATAÇÃO		**R$ 1.261.110,17**

2. FUNDAMENTAÇÃO DA CONTRATAÇÃO

2.1. Necessidade do Negócio

2.1.1. 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.

2.1.2. 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.

2.1.3. 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.

2.1.4. 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.

2.1.5. 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 ciberataques, que exploram as vulnerabilidades mais recorrentes de aplicações Web, têm crescido exponencialmente.

2.1.6. 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.

2.2. Justificativa da Contratação

2.2.1. 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.

2.2.2. 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.

2.2.3. Como dito acima, uma das funções realizada pela referida solução é o balanceamento de aplicações, responsável por realizar o balanceamento de aplicações 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.

2.2.4. 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.

2.2.5. 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.

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

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

2.3. Demonstrativo de resultados esperados com a solução:

a. Garantir que o acesso lógico aos ativos seja gerenciado e protegido, por meio de mecanismos de segurança de perímetro;
b. Tornar a infraestrutura da Justiça Eleitoral mais segura e confiável;
c. Prover resiliência ao ambiente de produção;
d. Assegurar a redundância adequada ao acesso de Sistemas hospedados pelo Tribunal.
e. Aumento da integridade, confiabilidade e disponibilidade dos serviços e informações;

2.4. Referências Legais

- 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.

2.5. Referências aos Estudos Técnicos

2.5.1. Processo SEI 0020437-45.2022.6.18.8000

a. Estudos Técnicos Preliminares - documento 1729580;

2.6. Classificação do Objeto

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

2.7. Relação entre a demanda **prevista** e a quantidade a ser registrada.

GRUPO ÚNICO	ITEM	DESCRIÇÃO	QTDE REGISTRADA	DEMANDA PREVISTA 2023	JUSTIFICATIVA
	1	Solução de *Web Application Firewall* (WAF), do tipo *appliance* físico com garantia e suporte de 60 meses	2	2	Cluster de proteção (2 *appliances*) das aplicação WEB hospedadas no ambiente de produção (Datacenter) do Tribunal, visando mitigar os riscos de ataque cibernético, com garantia e suporte técnico, pelo período de 60 (sessenta) meses, necessárias à manutenção da disponibilidade da solução.

	2	Serviço de Instalação e repasse de conhecimento *Hands-on*	1	1	Implantação da solução, incluindo instalação e configuração no ambiente do Tribunal e repasse técnico-operacional básico da solução
	3	Treinamento especializado	1	1	Capacitação da equipe técnica para administração da solução
	4	Banco de horas para suporte e consultoria	80hs	80hs	Supervisão da solução em produção após a implantação

3. ESPECIFICAÇÃO TÉCNICA MÍNIMA DA SOLUÇÃO

3.1. Características da Solução de *Web Application Firewall*

3.1.1. Os *appliances* físicos devem ser novos e de primeiro uso;

3.1.2. 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;

3.1.3. Devem ser novos, sem uso prévio e entregues em perfeito estado de funcionamento. Não devem ser remanufaturados, recondicionados ou possuir reparos de qualquer espécie;

3.1.4. Não serão aceitos equipamentos ou softwares que constem em anúncio ou lista do tipo *end-of-sale*, *end-of-support* ou *end-of-life* do fabricante, ou seja, produtos que serão descontinuados, perderão suporte e garantia oficiais do fabricante;

3.1.5. 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;

3.1.6. Os equipamentos serão instalados em rack com largura padrão de 19 polegadas, padrão EIA-310, ocupando no máximo 2Us do referido rack;

3.1.7. 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;

3.1.8. Devem ser fornecidos com todos os cabos de ligação lógica e elétrica necessários à instalação e perfeito funcionamento;

3.1.9. Dispor de fonte de alimentação redundante com tensão de entrada de 110V a 220V AC automática e frequência de 60Hz;

3.1.10. Possuir sistema operacional customizado especificamente para funções de *Web Application Firewall*, não podendo ser entregue appliance do tipo NGFW;

3.1.11. 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);

3.1.12. Possuir 01 interfaces 1GE, incluso interfaces de gerência com conectores padrão RJ45;

3.1.13. Todas as interfaces fornecidas devem estar licenciadas e habilitadas para uso imediato;

3.1.14. Possuir no mínimo de 8.000 Mbps de *throughput* em camada 7;

3.1.15. 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;

3.1.16. Recursos de agregação de portas baseado no protocolo LACP, segundo o padrão IEEE 802.3ad;

3.1.17. Memória RAM mínima de 16 GB;

3.1.18. Disco rígido com capacidade de armazenamento interno e retenção de logs para análise com capacidade mínima de 240GB;

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

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

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

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

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

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

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

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

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

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

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

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

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

3.1.32. Possuir suporte a IPv6;

3.1.33. 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;

3.1.34. Deve suportar, no mínimo, 1.000 VLANs simultaneamente;

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

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

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

3.1.38. O equipamento deverá permitir a sincronização das configurações:

- 3.1.38.1. De forma automática;
- 3.1.38.2. Manualmente, forçando a sincronização apenas no momento desejado.

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

- 3.1.39.1. Compartilhar a rede de *heartbeat* com a rede de dados;
- 3.1.39.2. Utilizar uma rede exclusiva para o *heartbeat*.

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

3.1.41. 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;

3.1.42. 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:

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

3.1.43. 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;

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

3.1.45. Permitir acesso *in-band* via SSH;

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

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

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

3.1.47. Manter internamente múltiplos arquivos de configurações do sistema;

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

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

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

3.1.51. Possuir Interface Gráfica via Web;

3.1.52. Possuir auto-complementação de comandos na CLI;

3.1.53. Possuir ajuda contextual;

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

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

3.1.55. A Solução deve ter suporte a sFlow;

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

3.1.57. Possuir, no mínimo, 3 (três) níveis de usuários na GUI – Super-Usuário, Usuário com permissões reduzidas, e usuário Somente Leitura;

3.1.58. 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;

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

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

3.1.61. Suportar a *rollback* de configuração salva e imagem;

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

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

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

3.1.65. A interface gráfica deverá permitir a reinicialização do equipamento;

3.1.66. Reinicialização do equipamento por comando na CLI;

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

3.1.68. Possuir *traps* SNMP;

3.1.69. Caso a solução possua suporte a RMON, deverá possuir suporte a monitoramento utilizando pelo menos 4 grupos: *statistics*, *history*, *alarms* e *events*;

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

3.1.71. Implementar *debugging*: CLI via console e SSH;

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

3.1.73. Permitir a criação de políticas diferenciadas por aplicação;

3.1.74. 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;

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

3.1.76. Permitir as seguintes opções de implementação:

3.1.76.1. Monitoramento (sem bloqueio);

3.1.76.2. Proxy (reverso e transparente).

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

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

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

3.1.80. 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;

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

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

3.1.82. 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*;

3.1.83. Com a finalidade de proteger as aplicações, a solução deve suportar proteções a JSON;

3.1.84. 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;

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

3.1.86. Bloqueio com intermediação e interrupção da conexão;

3.1.87. Criação de políticas automáticas que bloqueiam o endereço IP que realizar violações;

3.1.88. Utilização de página HTML informativa e personalizável como HTTP *Response* aos bloqueios;

3.1.89. Configuração de políticas de bloqueio baseadas em requisição HTTP, endereço IP e usuário de aplicação;

3.1.90. Identificar e armazenar o ataque acontecido com detalhes, com as seguintes informações:

3.1.90.1. Endereços IP que originaram os ataques;

3.1.90.2. Horário do ataque;

3.1.90.3. Nome do ataque;

3.1.90.4. Qual campo foi atacado;

3.1.90.5. Quantas vezes esse ataque foi realizado;

3.1.91. Possuir mecanismo de aprendizado automatizado capaz de identificar todos os conteúdos das aplicações;

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

3.1.93. Identificar ataques baseados em:

3.1.93.1. Regras;

3.1.93.2. Perfis de utilização;

3.1.93.3. Assinaturas e/ou comportamento.

3.1.94. Deve possuir tecnologia para mitigação de DDoS em camada 7 baseado em analise comportamental, usando o aprendizado;

3.1.95. A solução deve possuir a capacidade de capturar tráfego no formato TCP Dump, permitindo uma análise mais aprofundada por parte do administrador;

3.1.96. Detectar ataques de força bruta por meio dos seguintes métodos:

3.1.97. Aumento do tempo de resposta da aplicação monitorada ou bloqueio temporário do atacante;

3.1.98. Quantidade de transações por segundo (TPS), monitorando a quantidade de transações por segundo por endereço IP;

3.1.99. Detectar ataques do tipo força bruta em que:

3.1.99.1. O atacante solicita repetidamente o mesmo recurso;

3.1.99.2. O atacante realiza repetidas tentativas não autorizadas de acesso;

3.1.99.3. São utilizados ataques automatizados de login.

3.1.100. Detectar ataques do tipo força bruta que explorem:

3.1.100.1. Controles de acesso da aplicação (Erro 401 – *Unauthorized*);

3.1.100.2. Solicitações repetidas ao mesmo recurso, em qualquer parte/URL da aplicação;

3.1.100.3. Aplicações WEB que não retornam o Erro 401 (por meio da identificação de expressão regular no retorno/página de erro da aplicação);

3.1.100.4. Gerenciamento de sessão (muitas sessões de um único endereço IP ou a um *range* de IPs);

3.1.100.5. Clientes automatizados (robôs, requisições muito rápidas);

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

3.1.100.7. Possuir mecanismo para criação dinâmica de política de segurança, com aprendizado automático de padrão de utilização da aplicação, realizado sobre o fluxo de tráfego bidirecional atravessando o equipamento;

3.1.101. Apresentar proteção contra-ataques, como:

3.1.101.1. *Brute Force Login*;

3.1.101.2. *Buffer Overflow*;

3.1.101.3. *Cookie Injection*;

3.1.101.4. *Cookie Poisoning*;

3.1.101.5. *Cross Site Request Forgery* (CSRF);

3.1.101.6. *Cross Site Scripting* (XSS);

3.1.101.7. *Server Side Request Forgery* (SSRF)

3.1.101.8. *Directory Traversal*;

3.1.101.9. HTTP *Denial of Service*;

3.1.101.10. *Malicious Robots*;

3.1.101.11. *Parameter Tampering*;

3.1.101.12. SQL *Injection*;

3.1.101.13. Web *Services* (XML) *attacks*;

3.1.102. Permitir configurar granularmente, por aplicação protegida, restrições de métodos HTTP permitidos, tipos ou versões de protocolos, tipos de caracteres e versões utilizadas de *cookies*;

3.1.103. Suportar os seguintes critérios de decisão para realizar bloqueio ou gerar alerta, sendo que uma política pode conter um ou mais critérios simultaneamente:

3.1.103.1. Assinatura de ataque ou IPs de atacantes conhecidos;

3.1.103.2. Código de *response*;

3.1.103.3. Conteúdo da *cookie*;

3.1.103.4. Conteúdo do cabeçalho;

3.1.103.5. Conteúdo do *payload*;

3.1.103.6. *Hostname*;

3.1.103.7. IP de origem;

3.1.103.8. Método HTTP;

3.1.103.9. Número de ocorrências em determinado intervalo de tempo;

3.1.103.10. Parâmetro;

3.1.103.11. *User-agent* (navegador);

3.1.104. Deve proteger contra os seguintes ataque:

3.1.104.1. Ataques de negação de serviços automatizados;

3.1.104.2. *Worms* e vulnerabilidades conhecidas;

3.1.104.3. *Requests* em objetos restritos;

3.1.105. Deve proteger contra ataques SSRF (*Server Side Request Forgery*);

3.1.106. A solução oferecida deverá possuir proteção contra ataques, disponibilizando acesso a base de assinaturas e/ou atualizações periódicas até o fim do contrato;

3.1.107. 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;

3.1.108. Deve permitir que possa ser especificado na política os tipos de arquivos que serão bloqueados (*File Types*);

3.1.109. A solução deve permitir a inspeção de upload de arquivos para os servidores de aplicação, ou enviar para inspeção através do protocolo ICAP;

3.1.110. Deve possuir uma proteção proativa comportamental contra ataques automatizados por robôs e outras ferramentas de ataque;

3.1.111. Ao detectar uma condição de DDoS, assinaturas dinâmicas devem ser automaticamente criadas e implementadas em tempo real para proteção da aplicação;

3.1.112. A solução deve possuir proteção de DDoS L7 baseado em análise comportamental, sem precisar de nenhuma configuração manual;

3.1.113. Possuir método de mitigação de DoS L7 baseado em:

3.1.113.1. Descarte de todas as requisições de um determinado IP e/ou país suspeito;

3.1.113.2. Defesa proativa contra *Bot*, através da injeção de um desafio no Browser ou via Javascript para detectar se é um usuário legítimo ou robô.

3.1.114. Aprender o comportamento da aplicação:

3.1.114.1. Campos, valores e URLs;

3.1.115. Políticas sugeridas somente devem ser aplicadas após um período configurável ou possibilitar aplicá-las posteriormente;

3.1.116. 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*;

3.1.117. 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;

3.1.118. Proteger contra mensagens XML e SOAP malformadas;

3.1.119. Utilizar o campo HTTP X-*Forwarded-For* sem modificar seu conteúdo de origem, permitindo a diferenciação em ambientes com NAT;

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

3.1.121. 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;

3.1.122. Deverá permitir o cadastro de robôs que podem acessar a aplicação;

3.1.123. Deverá implementar proteção ao JSON (JavaScript *Object Notation*);

3.1.124. 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;

3.1.125. 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;

3.1.126. Deve proteger informações sensíveis e confidenciais da interceptação por terceiros, através da criptografia de dados. Deve proteger esses dados criptografados de *malwares* e *keyloggers*;

3.1.127. 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;

3.1.128. A solução deve fornecer relatórios consolidados de ataques com pelo menos os seguintes dados:

3.1.128.1. Resumo geral com as políticas ativas, anomalias e estatísticas de tráfego, Ataques DoS, Ataques de Força Bruta, Ataques de Robôs, Violações, URL, Endereços IP, Países, Severidade.

3.1.129. Deverá permitir o agendamento de relatórios a serem entregues por e-mail;

3.1.130. Emitir os seguintes relatórios gráficos dos ataques por:

3.1.130.1. Política de segurança;

3.1.130.2. Tipos de ataques;

3.1.130.3. Violações;

3.1.130.4. URL que foram atacadas;

3.1.130.5. Endereços IP de origem;

3.1.130.6. Localização geográfica dos endereços IPs de origem;

3.1.130.7. Severidade;

3.1.130.8. Código de resposta;

3.1.130.9. Métodos;

3.1.130.10. Protocolos;

3.1.130.11. Sessão;

3.1.131. Permitir a seleção de período para emissão dos relatórios;

3.1.132. Permitir a geração das seguintes informações, por período:

3.1.132.1. Permitir auditoria detalhada das alterações de configuração efetuadas, indicando usuário, ação e horário;

3.1.132.2. Informações estatísticas de quantidade de conexões completadas e bloqueadas;

3.1.132.3, Informações estatísticas de fluxo de tráfego;

3.1.133. Identificação, isolamento e bloqueio de ataques sofisticados para os protocolos: HTTP e HTTPS;

3.1.134. 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;

3.1.135. 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;

3.1.136. 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;

3.1.137. 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;

3.1.138. 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:

3.1.138.1. SSL *session cache timeout*;

3.1.138.2. *Session ticket*;

3.1.138.3. OCSP (*Online Certificate Status Protocol*) *Stapling*;

3.1.138.4. *Perfect forward secrecy*;

3.1.139. 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:

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

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

3.1.139.3. Ao realizar inspeção, proteção, *offload* e aceleração de tráfego criptografado através de SSL/TLS;

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

3.1.140. Deve possibilitar a customização da interface gráfica da página de login;

3.1.141. 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:

3.1.141.1. *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;

3.1.141.2. 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;

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

3.1.142. Deve suportar autenticação de múltiplos fatores utilizando *tokens* de Hardware ou *One-Time Passcode* (OTP);

3.1.143. Deve possuir capacidade para realizar *proxy* reverso com a finalidade de omitir a URI real, promovendo assim o acesso seguro às aplicações web internas;

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

3.1.144.1. DNS autoritativo;

3.1.144.2. DNS secundário;

3.1.144.3. DNS *resolver*;

3.1.144.4. DNS cache;

3.1.144.5. Balanceamento de DNS *servers*;

3.1.144.6. DNSSec;

3.1.145. Capacidade de uso de chave criptográfica para comunicação segura entre servidores DNS;

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

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

3.1.148. Deve ser capaz de gerar estatísticas sobre consultas de DNS por: aplicação, nome da *query*, tipo da *query*, endereço IP do cliente;

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

3.1.150. Deve prover as respostas a *queries* DNS da própria RAM CACHE;

3.1.151. A solução deve ser capaz de realizar IP *Anycast*;

3.1.152. A solução deve ser capaz de realizar DNSSec, independente da estrutura dos servidores DNS em uso;

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

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

3.1.154.1. *Round Robin*;

3.1.154.2. *Global Availability*;

3.1.154.3. Geografia;

3.1.154.4. *Least Connections*;

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

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

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

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

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

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

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

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

3.1.162.1. Por *cookie*;

3.1.162.2. Endereço de origem;

3.1.162.3. Sessão SSL;

3.1.162.4. Através de qualquer parâmetro do cabeçalho HTTP;

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

3.1.163. O equipamento oferecido deverá possuir monitores predefinidos ou possibilitar a configuração para, no mínimo, os seguintes protocolos:

3.1.163.1. ICMP, HTTP, HTTPS, Diameter, FTP, SASP, SMB, RADIUS, MSSQL, NNTP, ORACLE, RPC, LDAP, IMAP, SMTP, POP3, SIP, Real Server, SOAP, SNMP e WMI;

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

3.1.165. Realizar *Network Address Translation* (NAT);

3.1.166. Realizar proteção contra *syn flood*;

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

3.1.168. 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;

3.1.169. 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;

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

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

3.1.170. 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;

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

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

3.1.173. Possuir recursos para limitar o número de sessões estabelecidas com cada grupo de servidores;

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

3.1.175. Realizar *Network Address Translation* (NAT);

3.1.176. Realizar proteção contra *Denial of Service* (DoS);

3.1.177. Realizar proteção contra *Syn flood*;

3.1.178. Realizar limpeza de cabeçalho HTTP;

3.1.179. Deve possuir suporte a *Link Layer Discovery Protocol* (LLDP);

3.1.180. Suporte a otimização do protocolo TCP para ajustes a parâmetros das conexões clientes e servidor;

3.1.181. Deve ser capaz de realizar DHCP *relay*;

3.1.182. Deve possuir relatórios das aplicações, com pelos menos os seguintes gráficos:

3.1.182.1. Tempo de resposta da aplicação;

3.1.182.2. Latência;

3.1.182.3. Conexões para conjunto de servidores, servidores individuais;

3.1.182.4. Por URL;

3.1.182.5. A solução deve ter suporte a TLS 1.3.

3.2. Características do Serviço de Instalação e repasse de conhecimento *Hands-on*

3.2.1. Os serviços de instalação física, lógica serão executados pela CONTRATADA e deverão ser estruturados conforme as fases a seguir;

3.2.2. Fase de abertura:

3.2.2.1. Validar e homologar escopo do projeto;

3.2.2.2. Validar objetivos e premissas do projeto;

3.2.2.3. Validar riscos e restrições do projeto;

3.2.2.4. Identificar e validar os requisitos do projeto;

3.2.2.5. Efetuar o levantamento de informações sobre o ambiente atual, em complementação ao conjunto de informações apresentado nesta especificação técnica;

3.2.2.6. Efetuar o gerenciamento de mudanças, contemplando análise de riscos de implementação do sistema;

3.2.2.7. Apresentar o estudo dos riscos envolvidos na migração para o novo sistema a ser implantado.

3.2.3. Fase de planejamento:

3.2.3.1. Elaborar plano de projeto;

3.2.3.2. Definir as pessoas envolvidas por parte da CONTRATANTE no projeto;

3.2.3.3. Reunir as equipes da CONTRATADA e CONTRATANTE;

3.2.3.4. Definir os parâmetros de configuração básicos e avançados a serem implementados;

3.2.3.5. Apresentar o Mapa de rede contendo a topologia a ser implementada;

3.2.3.6. Apresentação do cronograma do projeto com os prazos e responsabilidades;

3.2.3.7. Verificar os pré-requisitos do projeto;

3.2.3.8. Apresentar plano do projeto para a homologação por parte da CONTRATANTE.

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

3.2.4.1. 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;

3.2.4.2. A CONTRATADA deverá efetuar instalação e configuração realizada de acordo com as recomendações do fabricante (*recommended settings*);

3.2.4.3. 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*);

3.2.4.4. Conexão e configuração de todos os equipamentos e/ou componentes da solução da rede do CONTRATANTE, inclusive configuração de VLANs e interfaces virtuais, se for o caso;

3.2.4.5. Atualização de softwares, firmwares e drivers que compõem a solução;

3.2.4.6. 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;

3.2.4.7. Aplicação das licenças necessárias à solução entregue;

3.2.4.8. Testes da solução, incluindo testes de *failover*;

3.2.4.9. Documentação do ambiente configurado e instalado.

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

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

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

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

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

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

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

3.2.11.1. O agrupamento dos "*appliances*" em configuração do tipo "cluster" do tipo ativo/ativo ou ativo/passivo;

3.2.11.2. Segmentação das redes por meio do uso de VLANs;

3.2.11.3. Definição das redes IP a serem empregadas pelos servidores reais (redes de serviço);

3.2.11.4. A criação de usuários para fins de operação e administração do sistema;

3.2.11.5. Configuração de alarmes e notificações automatizadas a serem enviadas via protocolos SNMP e/ou SMTP;

3.2.11.6. Configuração da topologia de conectividade de rede entre o sistema e os ativos de rede em operação nos datacenters do contratante;

3.2.11.7. Instalação, registro e ativação de licenças para todos os equipamentos ofertados, em total conformidade com essa especificação técnica;

3.2.11.8. Teste e homologação do conjunto de recursos e funcionalidades do sistema implantado.

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

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

3.2.13. O serviço de implantação da solução deverá ser concluído no prazo de, no máximo, 40(quarenta) dias, contados a partir da emissão do termo de recebimento provisório;

3.2.13.1. Para todos os efeitos, a conclusão dos serviços de instalação e configuração será atestada pela entrega do sistema em pleno funcionamento, incluindo documentação "*As Built*", contendo planejamento, relatório de instalação, configuração adotada, testes realizados e seus resultados, de acordo com as especificações do(s) fabricante(s) e demais condições estabelecidas nesta especificação técnica;

3.2.14. Características do repasse de conhecimento *hands-on*:

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

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

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

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

3.2.16. Condições de aceitação do repasse hands-on:

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

3.2.16.2. A não aceitação do *hands-on* implicará a na não aceitação da entrega definitiva do serviço (ITEM 2)

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

3.3. Treinamento especializado

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

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

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

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

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

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

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

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

3.3.4. A licitante deverá anexar a grade de treinamentos do fabricante, com a ementa do(s) curso(s), para comprovar que o(s)treinamento(s) ofertados cobrem os conhecimentos necessários para instalação, administração, configuração, gerência, otimização, resolução de problemas e utilização da solução;

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

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

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

3.3.8. O treinamento deverá ser ministrado por profissionais certificados pelo fabricante, cuja comprovação deverá ser encaminhada na assinatura do Contrato;

3.3.9. A contratada deverá fornecer material didático individual, na modalidade digital, que abranja todo o conteúdo do(s) curso(s). Todo o material didático oferecido pela Contratada para realização do treinamento, atualizado e poderá estar em inglês ou português;

3.3.10. O treinamento deve ser ministrado em português do Brasil. Caso não exista material oficial do produto em língua portuguesa, será aceito material em inglês;

3.3.11. O treinamento deverá oferecer acesso a laboratório prático virtual, fornecido pela contratada, para configuração e execução de exercícios práticos;

3.3.11.1. No ambiente de treinamento, os servidores indicados pelo CONTRATANTE devem ter acesso em ambiente de laboratório a todos os produtos ofertados (ou similares) para realização da capacitação;

3.3.12. A Contratada deverá emitir para o servidor participante, sem ônus para o Tribunal e no prazo máximo de até 10 (dez) dias úteis após o término do treinamento, o certificado de conclusão, no qual deverá constar o nome do treinando, a data, o local e a carga horária. A cópia deste certificado deverá acompanhar a nota fiscal/fatura para o devido pagamento;

3.3.13. A ausência do servidor ao treinamento é de responsabilidade do Tribunal, cabendo à contratada informar no certificado a carga horária e assiduidade do servidor;

3.3.14. A Contratada deverá aplicar o Formulário de Satisfação, conforme modelo de formulário constante no Anexo III deste Termo de Referência:

3.3.14.1. 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 ser considerado proveitoso;

3.3.14.2. 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) dos 07(sete) itens avaliados;

3.3.14.3. Caso o resultado da Avaliação de Instrutor seja considerado “não proveitoso”, o treinamento fornecido será considerado não aceito;

3.3.14.4. 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;

3.3.14.5. Na hipótese de o resultado do segundo treinamento ser “não proveitoso”, o objeto será considerado não aceito, aplicando-se as sanções previstas contratualmente

3.4. Banco de horas para suporte e consultoria

3.4.1. Crédito de horas técnicas para a prestação de serviços de suporte especializado e consultoria, após a conclusão da instalação, configuração e treinamento da solução ofertada;

3.4.2. Os serviços de suporte especializado e consultoria deverão abranger, mas não se limitando, a demandas de administração, operação assistida, planejamento e *tuning*, detecção e correção de erros, apoio à operação, análise de desempenho, ajustes, recomendação de boas práticas, reconfiguração e integração com outros sistemas do ambiente da CONTRATANTE;

3.4.3. O banco de horas técnicas poderá ser utilizado em até 12 (doze) meses e deverá ter tempo de resposta de até 04 (quatro) horas;

3.4.4. As horas técnicas poderão ser utilizadas em dias consecutivos ou alternados e serão contabilizados em termos de homem/hora;

3.4.5. As horas técnicas serão consumidas sob demanda, de acordo com as necessidades da CONTRATANTE;

3.4.6. Os serviços técnicos especializados poderão ser executados presencial ou remotamente;

3.4.7. Para a execução dos serviços técnicos especializados, a CONTRATANTE elaborará documento de escopo do serviço a ser realizado com as entregas que deverão ser alcançadas e, em comum acordo com a CONTRATADA, definirá a quantidade de horas estimadas, os prazos de execução com datas de início e encerramento do atendimento;

3.4.8. Qualquer alteração na quantidade de horas previstas para a realização da demanda deverá ser justificada e previamente aprovada pela CONTRATANTE;

3.4.9. Os serviços serão realizados utilizando o regime de 8x5 para atendimentos programados. Para atendimentos emergenciais e fora do horário comercial, em regime 24x7, serão computadas horas em dobro;

3.4.10. A CONTRATADA deverá produzir, como resultado de cada atendimento técnico realizado, um Relatório de Atendimento Técnico - RAT, contendo no mínimo as seguintes informações:

3.4.10.1. Discriminação das atividades executadas;

3.4.10.2. Resultados obtidos;

3.4.10.3. Conclusões técnicas e sugestões para melhoria do ambiente;

3.4.10.4. Total de horas utilizadas, contendo o início, interrupções e final do atendimento.

3.4.11. A CONTRATADA deverá entregar o RAT à CONTRATANTE, no prazo máximo de 2 (dois) dias úteis, após a conclusão dos serviços;

3.4.12. O serviço será considerado concluído após o aceite da CONTRATANTE;

3.4.13. A CONTRATANTE emitirá aceite de prestação de suporte técnico, após a conclusão do serviço, condicionado à verificação de conformidade do serviço executado;

3.4.14. O faturamento dos serviços técnicos utilizados será realizado mensalmente e considerará os chamados abertos e concluídos dentro do mês de referência.

4. APRESENTAÇÃO DA PROPOSTA E CRITÉRIO DE JULGAMENTO

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

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

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

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

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

4.6. A proposta deve certificar que nenhum dos equipamentos fornecidos contenha substâncias perigosas como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr(VI)), cádmio (Cd), bifenil polibromados (PBBs), éteres difenil-polibromados (PBDEs) em concentração acima da recomendada na diretiva RoHS (*Restriction of Certain Hazardous Substances*), sendo que para efeitos de avaliação das propostas e aceitação do produto deverá ser fornecido certificação emitida por instituição credenciada pelo INMETRO ou por documentação oficial do fabricante; sendo aceito ainda, a comprovação deste requisito por intermédio da certificação EPEAT (www.epeat.net), se houver referência no referido site para a solução de TI associada ao objeto.

4.7. A proposta deverá possuir validade mínima de 90 (noventa) dias.

4.8. Os preços, na proposta deverão ser fornecidos da seguinte forma:

	ITEM	DESCRIÇÃO	QTDE REGISTRADA	VALOR UNITÁRIO	VALOR TOTAL
GRUPO ÚNICO	1	Solução de *Web Application Firewall* (WAF), do tipo *appliance* físico com garantia e suporte de 60 meses	2		
	2	Serviço de Instalação e repasse de conhecimento Hands-on	1		
	3	Treinamento especializado	1		
	4	Banco de horas para suporte e consultoria	80hs		
	VALOR GLOBAL DO GRUPO				

4.9. A classificação das propostas será pelo critério do **MENOR PREÇO POR GRUPO.**

4.10. Os valores dos lances deverão ter o intervalo mínimo de R$ 1.000,00 (um mil reais), para o GRUPO Único do Pregão (Parágrafo único do artigo 31, do Decreto nº 10.024/2019).

4.11. Será adotado para o envio de lances o modo de disputa "aberto", em que os licitantes apresentarão lances públicos e sucessivos, com prorrogações.

5. ESTRATÉGIA DA CONTRATAÇÃO

5.1. Regime, Tipo e Modalidade da Licitação

5.1.1. O objeto deste Termo de Referência terá grupo único e não será parcelado, uma vez que todos os produtos e serviços a serem fornecidos e prestados são componentes de uma única solução de TI, a qual não pode ser desmembrada sem que haja perda de produtividade e economia de escala.

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

5.1.3. O prazo de vigência da garantia dos itens que compõem a solução será conforme tabela a seguir:

GRUPO ÚNICO	ITEM	DESCRIÇÃO	GARANTIA (MESES)
	1	Solução de *Web Application Firewall* (WAF), do tipo *appliance* físico	60

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

5.2. Da aplicação de direitos de preferência

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

5.3. Critérios de julgamento das propostas

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

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

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

5.4. Critérios de qualificação técnica para a habilitação

5.4.1. A LICITANTE deverá apresentar atestado(s) de capacidade técnica, fornecido(s) por pessoa jurídica de direito público ouprivado, que comprove o fornecimento e implantação de, pelo menos, 01 (um) appliance virtual e/ou físico da solução *Web Application Firewall* (WAF), a fim de comprovar a aptidão para desempenho de atividade pertinente e compatível com o objeto dalicitação;

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

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

5.4.4. Será aceito o somatório de atestados e/ou declarações para comprovar a experiência mínima exigida, porém os períodos concomitantes serão computados uma única vez;

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

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

5.5. Documentação exigida - fase de assinatura do contrato

5.5.1. A CONTRATADA deverá apresentar após assinatura do contrato, no prazo de até 15 (quinze) dias úteis contados da publicação do extrato do Contrato no Diário Oficial da União, a documentação associadas ao(s) profissional(is) envolvidos e certificações mínimas associadas à execução dos serviços, conforme os itens a seguir;

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

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

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

5.5.5. Após o recebimento do pedido de instalação, a contratada terá 10 (dez) dias úteis para informar o técnico que fará a instalação acompanhada da comprovação da certificação exigida;

5.6. Dotação orçamentária

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

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

5.7. Critérios sociais e culturais

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

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

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

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

5.8. Manutenção de sigilo e normas de segurança

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

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

6. DEFINIÇÃO DAS OBRIGAÇÕES CONTRATUAIS

6.1. Definição das obrigações da contratante

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

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

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

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

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

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

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

6.1.1.7. Atestar a(s) notas fiscal(ais) apresentada(s) pela CONTRATADA após o recebimento definitivo dos equipamentos, conforme especificações descritas neste Termo de Referência.

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

6.1.1.9. Prestar informações e esclarecimentos que venham a ser solicitados pela CONTRATADA, necessários à execução do contratado.

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

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

6.2. Definição das obrigações da contratada

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

6.2.1. 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;

6.2.2. Atender aos chamados técnicos no prazo estipulado pela contratante;

6.2.3. 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);

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

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

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

6.2.7. Apresentar o Termo de Compromisso e Manutenção de Sigilo (Anexo I) e Termo de Ciência (Anexo II) dos envolvidos na implantação da solução, migração de dados e operação assistida.

6.2.8. Prover assistência técnica no território brasileiro.

6.2.9. Dar garantia não inferior a 60 (sessenta) meses, a contar da data de emissão do Termo de Recebimento Definitivo.

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

6.2.11. Comunicar à Contratante, no prazo máximo **de 01 dia útil** que antecede a data da entrega do material/serviço, os motivos que impossibilitem o cumprimento do prazo ajustado, com a devida comprovação;

6.2.11.1. Eventual pedido de prorrogação deverá ser encaminhado para o seguinte endereço: Seção de Infraestrutura do Tribunal Regional Eleitoral do Piauí, Praça Des. Edgar Nogueira, S/N – Centro Cívico, Bairro Cabral, Teresina-PI, CEP 64000-920, fone: (086) 2107-9756 e-mail: seinf@tre-pi.jus.br;

6.2.11.2. Em casos excepcionais, autorizados pelo Contratante, o documento comprobatório do alegado poderá acompanhar a entrega do produto;

7. EXECUÇÃO DO CONTRATO

7.1. Prazo de entrega

7.1.1. O prazo de entrega dos materiais será de, no máximo, 90 dias corridos, a contar da publicação do contrato.

7.1.2. O prazo de conclusão dos serviços associados ao item 2 (Serviço de Instalação e repasse de conhecimento *hands-on*) será de, no máximo, 40 (quarenta) dias corridos, a contar da data do recebimento provisório dos bens fornecidos.

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

7.2. Local de execução/entrega

7.2.1. A **entrega do material** ocorrerá na Sede do Tribunal Regional Eleitoral, localizada na Praça Des. Edgar Nogueira, s/n, Cabral, Teresina-PI - CEP 64.000-920.

7.2.2. Os **serviços poderão ser executados**, a critério da Contratante, na Sede do Tribunal ou no Fórum dos Cartórios das Zonas Eleitorais da Capital, localizado na Av. Marechal Castelo Branco, 1377, Cristo Rei, Teresina-PI - CEP 64.014-058.

7.3. Condições gerais do fornecimento

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

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

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

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

7.3.5. O fornecedor deverá apresentar a garantia correspondente a cada item da Ata de Registro de Preços, a contar da data de aceite efetuada pelo TRE-PI.;

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

8. FORMA DE PAGAMENTO

8.1. O pagamento será realizado em até 10 (dez) dias úteis a contar do atesto da Nota Fiscal, salvo quando houver pendência de liquidação de qualquer obrigação financeira que for imposta à CONTRATADA, em virtude de penalidade ou inadimplência, depois do aceite na nota fiscal e conclusão da entrada de material efetuada pela Fiscalização do TRE-PI, por meio de depósito em conta corrente, mediante Ordem Bancária.

8.2. A Nota Fiscal deverá ser apresentada devidamente preenchida e discriminada, em nome do Tribunal Regional Eleitoral do Piauí, CNPJ nº 05.957.363/0001-33 e remetida via protocolo ao setor solicitante.

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

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

8.5. O pagamento será efetuado somente após concluídas as fases de entrega de material e serviços de instalação associados ao objeto.

8.6. Nos casos de eventuais atrasos de pagamento provocados exclusivamente pela Administração, o valor devido deverá ser acrescido de atualização financeira, e sua apuração se fará desde a data de seu vencimento até a data do efetivo pagamento, em que os juros de mora serão calculados à taxa de 0,5% (meio por cento) ao mês, ou 6% (seis por cento) ao ano, mediante aplicação das seguintes fórmulas:

$$I = \frac{(TX/100)}{365}$$

EM = I x N x VP, onde:

I = Índice de atualização financeira;

TX = Percentual da taxa de juros de mora anual;

EM = Encargos moratórios;

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

VP = Valor da parcela em atraso.

8.7. Havendo erro na apresentação da Nota Fiscal ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, como, por exemplo, obrigação financeira pendente, decorrente de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que a Contratada providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a Contratante.

8.8. 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.

9. GESTÃO DO CONTRATO

9.1. Fases associadas à execução do objeto

9.1.1.As fases e prazos referentes à execução do objeto estão consolidados na tabela a seguir:

ITEM	FASE ASSOCIADA	PREVISÃO	PRAZO
1	Entrega dos bens contratados (Item 1) deste Termo de Referência (contratada)	7.1.1	90 (noventa) dias corridos, a contar da publicação do contrato
2	Emissão do termo de recebimento provisório dos bens contratados (Item 1) (contratante)	9.3.1	05 (cinco) dias corridos, após a entrega dos bens
3	Entrega da documentação dos profissionais envolvidos (contratada)	5.5.1	15 (quinze) dias corridos após publicação do extrato do contrato no D.O.U.
4	Conclusão da implantação da solução (Item 2)	3.2.13/7.1.2	40 (quarenta) dias corridos, após a emissão do termo de recebimento provisório
5	Emissão do termo de recebimento definitivo	9.4.1	10 (dez) dias corridos após a conclusão da implantação da solução

9.2. Do recebimento provisório e definitivo

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

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

9.2.3. Os bens poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser substituídos no prazo de 20 (vinte) dias corridos, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades.

9.3. Termo de recebimento provisório

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

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

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

9.4. Termo de recebimento definitivo

9.4.1. Os representantes da administração deverão, **no prazo de 10 dias corridos da conclusão da implantação da solução**, conferir a qualidade e especificações funcionais dos equipamentos entregues e confrontá-las com as exigências editalícias, promoverem testes de desempenho (se for o caso), verificar licenças, registrar a data de entrega, emitir o recibo e o termo de recebimento definitivo, bem como registrar quaisquer ocorrências que impactem na avaliação da qualidade do fornecimento pela LICITANTE VENCEDORA.

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

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

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

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

10. SANÇÕES ADMINISTRATIVAS

10.1. 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, sem prejuízo das multas previstas neste Termo e das demais cominações legais, aquele que:

a. Deixar de entregar a documentação exigida no Edital;
b. Convocada dentro do prazo de validade de sua proposta, não assinar Ata de Registro de Preços/contrato;
c. Apresentar documento falso ou fizer declaração falsa;
d. Ensejar o retardamento da execução do objeto do contrato;
e. Não mantiver a proposta, injustificadamente;
f. Falhar ou fraudar na execução do contrato;
g. Comportar-se de modo inidôneo;
h. Cometer fraude fiscal.

10.2. Sem prejuízo das demais sanções previstas no Art. 87 da Lei n.º 8.666/93, pela inexecução total ou parcial do objeto deste Termo de Referência, a Administração do Tribunal Regional Eleitoral do Piauí, poderá, garantida a defesa prévia, aplicar à licitante vencedora as seguintes sanções:

10.2.1. Advertência, nas hipóteses de faltas leves, assim entendidas aquelas que não acarretem prejuízos para o TRE/PI;

10.2.2. Multa compensatória de até 10% (dez por cento) sobre o valor global da Ata de Registro de Preços, na hipótese de recusa em assinar a Ata de Registro de Preços ou do contrato, na hipótese de recusa em assinar o instrumento de contrato;

10.2.3. Multa compensatória de até 10% (dez por cento) sobre o valor do contrato, na hipótese de inexecução parcial ou total da obrigação;

10.2.4. Multa moratória de 0,2% (dois décimos por cento) sobre o valor do contrato por dia de atraso na entrega do material e/ou conclusão do serviço contratado, limitado a 10% (dez por cento).

10.2.5. **Suspensão temporária** de participação em licitação e impedimento de contratar com o TRE-PI, se, por culpa ou dolo, prejudicar ou tentar prejudicar a execução do Contrato, nos seguintes prazos e situações:

Por até 1 (um) ano	• 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;
Por até 2 (dois) anos	• 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, sem prejuízo das demais medidas cabíveis.

10.2.6. **Declaração de inidoneidade** quando constatada má-fé, ações intencionais com prejuízos para o TRE-PI, atuação com interesses escusos, reincidência em faltas que acarretem prejuízo ao TRE-PI ou aplicações anteriores de sucessivas outras sanções, implicando proibição da CONTRATADA de transacionar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, podendo ser aplicada, dentre outros casos, quando:

a) Tiver sofrido condenação definitiva por ter praticado, por meios dolosos, fraude fiscal no recolhimento de quaisquer tributos;

b) Praticar atos ilícitos, visando a frustrar os objetivos da licitação;

c) Demonstrar, a qualquer tempo, não possuir idoneidade para licitar ou contratar com o TRE-PI, em virtude de atos ilícitos praticados.

10.3. Não será aplicada multa de valor igual ou inferior a 10% (dez por cento) da quantia definida na Portaria nº 75, de 22 de março de 2012, do Ministério da Fazenda, ou em norma que vier a substituí-la, para inscrição de débito na Dívida Ativa da União.

10.3.1 As aplicações de penalidades que recaiam no subitem 10.3. poderão ser convertidas em advertência por escrito, a critério da Administração Superior.

10.3.2 Não se aplica o disposto no *caput* deste subitem, quando verificada, em um período de 02 (dois) anos, contados do registro da penalidade no SICAF, a ocorrência de multas que somadas ultrapassem o valor fixado para inscrição em Dívida Ativa da União.

10.4. No caso de não-recolhimento do valor da multa dentro do prazo estipulado na GRU, serão acrescidos juros moratórios de 0,03% ao dia até o prazo máximo de **15 (quinze) dias** e, não sendo recolhida, a multa será convertida em suspensão de licitar com o TRE-PI e o valor devido ou a diferença ainda não recolhida aos cofres públicos será objeto de inscrição na Dívida Ativa da União, de acordo com a legislação em vigor.

10.5. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à CONTRATADA, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente a Lei nº 9.784, de 1999.

10.6. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

10.7. As multas a que se referem os itens acima serão descontadas dos pagamentos devidos pelo TRE-PI ou cobradas diretamente da Adjudicatária, amigável ou judicialmente, e poderão ser aplicadas cumulativamente com as demais sanções previstas neste tópico.

10.8. As penalidades serão precedidas de notificação e obrigatoriamente registradas no SICAF e, no caso de suspensão temporária e impedimento de licitar, estas deverão ser publicadas no Diário Oficial da União e o adjudicatário deverá ser descredenciado pelo período indicado pelo Gestor, após observado o devido contraditório e a ampla defesa, sem prejuízo das multas previstas neste Termo.

10.9. Os atos lesivos praticados pela adjudicatária serão objeto de apuração e, portanto, passíveis de responsabilização administrativa visando à aplicação das sanções previstas no art. 6º da Lei nº 12.846/2013, não afastando a possibilidade de sua responsabilização na esfera judicial.

11. DA GARANTIA E DO SUPORTE TÉCNICO

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

11.1.1. A vigência da garantia começará a contar a partir do recebimento definitivo;

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

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

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

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

11.5. Qualquer software ou equipamento com hardware defeituoso, peças quebradas, com defeito ou gastas pelo uso normal deverá ser substituído por outro de mesma marca e modelo e com as mesmas características técnicas ou superiores, novo e de primeiro uso, no prazo de 72 (setenta e duas) horas a partir de notificação do CONTRATANTE;

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

11.7. Suporte Técnico durante o período de Garantia Técnica:

11.7.1. 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;

11.7.2. 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;

11.7.3. 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;

11.7.4. 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;

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

11.7.6. 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;

11.7.7. 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 em Brasília por todo o período da garantia técnica;

11.7.8. 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;

11.7.9. 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;

11.7.10. 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;

11.7.11. 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;

11.7.12. 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.

12. VIGÊNCIA DA ATA DE REGISTRO DE PREÇOS E DO CONTRATO

12.1. O prazo de vigência da ata deverá abranger um período de **12 (doze) meses**, contados a partir da data de sua publicação.

12.1.1. A assinatura da ata poderá ocorrer digitalmente, através de cadastramento prévio no SEI, por servidor autorizado por este Regional, consoante disposto no art. 16, da instrução Normativa TRE-PI nº 01/2018.

12.2. A vigência do contrato decorrente da ata de registro de preços formalizada será de **60 (sessenta) meses a contar da emissão do termo de recebimento definitivo da solução**.

13. ADESÃO À ATA DE REGISTRO DE PREÇOS

13.1. Conforme Item 5.1.4, será permitida a adesão aos Tribunais Regionais Eleitorais que não figuram como partícipes desta Ata de Registro de Preços, em razão da arquitetura proposta na Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).

14. ÓRGÃO GERENCIADOR E ÓRGÃOS PARTICIPANTES

14.1. Caberá ao TRE-PI, órgão gerenciador, a prática de todos os atos de controle e administração do Sistema de Registro de Preços previstos no art. 5º do Decreto nº 7.892/2013 e suas alterações, especificamente o que segue:

14.1.1. Disponibilizar a Ata de Registro de Preços aos órgãos participantes;

14.1.2. Gerenciar a Ata de Registro de Preços;

14.1.3. Conduzir eventuais negociações dos preços registrados;

14.1.4. aplicar, garantida a ampla defesa e o contraditório, as penalidades decorrentes de infrações no procedimento licitatório;

14.1.5. aplicar, garantida a ampla defesa e o contraditório, as penalidades decorrentes do descumprimento do pactuado na Ata de Registro de Preços ou do descumprimento das obrigações contratuais, em relação às suas próprias contratações; e

14.1.6. fazer o controle permanente da variação dos preços do mercado, de forma a comprovar que os preços registrados permanecem compatíveis com os praticados no mercado.

14.2. Os Órgãos interessados em participar da Intenção de Registro de Preços se manifestarão diretamente no sistema ComprasNet;

14.3. O TRE-PI consolidará as informações relativas à estimativa individual e total de consumo, listando os participantes neste edital;

15. LEI GERAL DE PROTEÇÃO DE DADOS

15.1. Em observância ao disposto na Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais:

15.1.1. É vedada às partes a utilização de todo e qualquer dado pessoal, repassado em decorrência da execução contratual, para finalidade distinta da contida no objeto da contratação, sob pena de responsabilização administrativa, civil e criminal.

15.1.2. Para fins de execução do objeto contratado e de cumprimento de obrigação legal ou regulatória, o Contratante poderá proceder ao tratamento dos dados pessoais dos representantes legais da Contratada, inclusive para publicação nos portais de Transparência do Contratante.

15.1.3. Selecionada a empresa a ser contratada, para fins de assinatura do instrumento contratual, o representante legal da empresa e titular dos dados pessoais será cientificado do tratamento de seus dados a ser realizado pelo Contratante, na forma da Declaração de Concordância e Veracidade, conforme modelo constante na minuta de contrato.

16- DISPOSIÇÕES GERAIS

16.1. Quaisquer dúvidas acerca do pleito poderão ser esclarecidas pela SEINF– Seção de Infraestrutura deste Tribunal (telefones (86) 2107-9679 ou 2107-9816), em dias úteis, no horário das 8:00 às 15:00 horas, que funcionam na sede do Tribunal, situada na Praça Des. Edgard Nogueira, s/n, Bairro: Cabral, em Teresina-PI, CEP: 64.000-

830.

16.2. Nenhuma indenização será devida às empresas por apresentarem documentação e/ou elaborarem proposta relativa ao presente Termo de Referência.

16.3. Na contagem dos prazos estabelecidos, excluir-se-á o dia do início e incluir-se-á o do vencimento. Vale ressaltar que somente se iniciam e vencem os prazos em dias de expediente no TRE-PI.

16.4. As empresas são responsáveis pela fidelidade e legitimidade das informações e dos documentos apresentados em qualquer época ou fase em decorrência deste Termo.

16.5. Deverá ser respeitado o disposto na Res. n.º 07/2005 do Conselho Nacional de Justiça.

16.6. São partes integrantes deste Termo de Referência:

ANEXO I - TERMO DE COMPROMISSO E MANUTENÇÃO DE SIGILO

ANEXO II - TERMO DE CIÊNCIA

ANEXO III - AVALIAÇÃO DO TREINAMENTO ESPECIALIZADO

ANEXO IV - PLANILHA DE FORMAÇÃO DE PREÇOS

ANEXO V – DECLARAÇÃO DE CONCORDÂNCIA E VERACIDADE

ANEXO I

TRIBUNAL REGIONAL ELEITORAL DO PIAUÍ

PRAÇA DESEMBARGADOR EDGARD NOGUEIRA. S/Nº - CENTRO CÍVICO - BAIRRO CABRAL - CEP 64000920 - TERESINA - PI

TERMO DE COMPROMISSO E MANUTENÇÃO DE SIGILO

A **<EMPRESA>**, pessoa jurídica com sede em **<MUNICÍPIO>** , inscrita no CNPJ/MF com o nº **<CNPJ>**, neste ato representada na forma de seus atos constitutivos, doravante denominada simplesmente **CONTRATADA**, por tomar conhecimento de informações sobre o ambiente computacional da Justiça Eleitoral do Piauí, aceita as regras, condições e obrigações constantes do presente Termo.

O objetivo deste Termo de Compromisso e Manutenção de Sigilo é prover a necessária e adequada proteção às informações restritas de propriedade exclusiva do TRE-PI reveladas à CONTRATADA em função da prestação dos serviços objeto do contrato nº ___/20___.

A expressão "informação restrita" abrangerá toda informação escrita, oral ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: técnicas, projetos, especificações, desenhos, cópias, diagramas, fórmulas, modelos, amostras, fluxogramas, croquis, fotografias, plantas, programas de computador, discos, disquetes, pen drives, fitas, contratos, planos de negócios, processos, projetos, conceitos de produto, especificações, amostras de idéia, clientes, nomes de revendedores e/ou distribuidores, preços e custos, definições e informações mercadológicas, invenções e idéias, outras informações técnicas, financeiras ou comerciais, dentre outras.

A CONTRATADA compromete-se a não reproduzir nem dar conhecimento a terceiros, sem a anuência formal e expressa do TRE-PI, das informações restritas reveladas.

A CONTRATADA compromete-se a não utilizar, bem como a não permitir que seus diretores, consultores, prestadores de serviços, empregados e/ou prepostos utilizem, de forma diversa da prevista no contrato de prestação de serviços ao TRE-PI- as informações restritas reveladas.

A CONTRATADA deverá cuidar para que as informações reveladas fiquem limitadas ao conhecimento dos diretores, consultores, prestadores de serviços, empregados e/ou prepostos que estejam diretamente envolvidos nas discussões, análises, reuniões e demais atividades relativas à prestação de serviços ao TRE-PI, devendo cientificá-los da existência deste Termo e da natureza confidencial das informações restritas reveladas.

A CONTRATADA firmará acordos por escrito com seus diretores, consultores, prestadores de serviços, empregados e/ou prepostos cujos termos sejam suficientes a garantir o cumprimento de todas as disposições do presente Termo.

A CONTRATADA obriga-se a informar imediatamente ao TRE-PI qualquer violação das regras de sigilo estabelecidas neste Termo de que tenha tomado conhecimento ou ocorrido por sua ação ou omissão, independentemente da existência de dolo.

A quebra do sigilo das informações restritas reveladas, devidamente comprovadas, sem autorização expressa do TRE-PI, possibilitará a imediata rescisão de qualquer contrato firmado entre o TRE-PI e a CONTRATADA sem qualquer ônus para o TRE-PI. Nesse caso, a CONTRATADA estará sujeita ao pagamento ou recomposição de todas as perdas e danos sofridos pelo TRE-PI, advindos de sua ação ou omissão, inclusive os de ordem moral, bem como os de responsabilidade civil e criminal, os quais serão apurados em regular processo judicial ou administrativo.

O presente Termo tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de acesso às informações restritas do TRE-PI. E, por aceitar todas as condições e obrigações constantes deste documento, a CONTRATADA assina o presente Termo através de seus representantes legais.

Teresina, ____ de _____ de 2023.

[NOME DA CONTRATADA]

_____

[Nome legível do Representante Legal]

ANEXO II

TRIBUNAL REGIONAL ELEITORAL DO PIAUÍ

PRAÇA DESEMBARGADOR EDGARD NOGUEIRA. S/Nº - CENTRO CÍVICO - BAIRRO CABRAL - CEP 64000920 - TERESINA - PI

TERMO DE CIÊNCIA

CONTRATO Nº:
OBJETO: Registro de preços para eventual e futura aquisição de **Solução de *Web Application Firewall*** (WAF) e balanceamento de carga, incluindo serviços de implantação, transferência tecnológica (*hands-on*), treinamento especializado, operação assistida e garantia da solução por 60 (sessenta) meses

CONTRATADA:
CNJP:
Representante da Contratada:
CPF:

Representante da Contratada:
CPF:

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

■ Ter plena ciência e conhecimento do Termo de Compromisso e Manutenção de Sigilo firmado pela CONTRATADA;

■ Ter conhecimento de sua(s) responsabilidade(s) no que concerne ao sigilo que deverá ser mantido sobre as atividades desenvolvidas ou as ações realizadas no âmbito do Contrato Administrativo:

■ Comprometer-se a guardar sigilo necessário sobre todas as informações que eventualmente venha(m) a tomar conhecimento;

■ Comprometer-se a prestar obediência às políticas de segurança da informação vigentes no Tribunal Regional Eleitoral do Piauí ou que poderão ser instituídas durante a vigência do contrato.

IDENTIFICAÇÃO E ASSINATURA DO(S) DECLARANTE(S)

Nome:			
CPF:		Função/Cargo:	
Assinatura:			

Nome:			
CPF:		Função/Cargo:	
Assinatura:			

Nome:			
CPF:		Função/Cargo:	
Assinatura:			

Teresina, ____ de _____ de 2022.

[NOME DA CONTRATADA]

_____
[Nome legível do Representante Legal]

ANEXO III

TRIBUNAL REGIONAL ELEITORAL DO PIAUÍ

PRAÇA DESEMBARGADOR EDGARD NOGUEIRA. S/Nº - CENTRO CÍVICO - BAIRRO CABRAL - CEP 64000920 - TERESINA - PI

AVALIAÇÃO DO TREINAMENTO ESPECIALIZADO

Curso:	
Promotor:	
Período:	
Carga Horária:	
Instrutor:	
Objetivo:	

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

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

I - PROMOTOR DO EVENTO	**NOTA**			
ITEM	1	2	3	4
1 - Quanto à organização do evento				
2 - Quanto à adequação das instalações				
3 - Quanto à adequação dos recursos audiovisuais				
4 - Quanto à qualidade do material didático				
II - CONTEÚDO PROGRAMÁTICO	**NOTA**			
ITEM	1	2	3	4
1 - Quanto ao cumprimento do conteúdo programático				
2 - Quanto ao detalhamento na abordagem dos tópicos				
3 - Quanto à adequação da carga horária				
4 - Quanto a adequação do conteúdo a sua necessidade de conheci				
III - INSTRUTOR	**NOTA**			
ITEM	1	2	3	4
1 - Quanto ao domínio do assunto				
2 - Quanto à relevância e atualidade dos conhecimentos difundidos				
3 - Quanto à promoção de um ambiente favorável à aprendizagem				
4 - Quanto à clareza e objetividade nas exposições				
5 - Quanto à objetividade na administração do tempo				
6 - Quanto ao incentivo à participação da turma				
7 - Quanto a disponibilidade para o atendimento e o apoio aos alunos				
IV - APROVEITAMENTO	**NOTA**			
ITEM	1	2	3	4
1 - Quanto á assimilação do conteúdo				
2 - Quanto à adequação do conteúdo ao objetivo proposto por sua unidade de lotação				
V - COMENTÁRIOS E SUGESTÕES				

ANEXO IV

TRIBUNAL REGIONAL ELEITORAL DO PIAUÍ

PRAÇA DESEMBARGADOR EDGARD NOGUEIRA. S/Nº - CENTRO CÍVICO - BAIRRO CABRAL - CEP 64000920 - TERESINA - PI

PLANILHA DE FORMAÇÃO DE PREÇOS

GRUPO ÚNICO	ITEM	DESCRIÇÃO	QTDE REGISTRADA	VALOR UNITÁRIO	VALOR TOTAL
	1	Solução de *Web Application Firewall* (WAF), do tipo *appliance* físico com garantia e suporte de 60 meses	2	R$ 570.198,38	R$ 1.140.396,76
	2	Serviço de Instalação e repasse de conhecimento Hands-on	1	R$ 46.988,17	R$ 46.988,17

	3	Treinamento especializado	1	R$ 45.362,50	R$ 45.362,50
	4	Banco de horas para suporte e consultoria	80hs	R$ 354,53	R$ 28.362,75
	VALOR GLOBAL DO GRUPO				**R$ 1.261.110,17**

*Valores alcançados conforme Planilha de Formação de Preços (SEI 1770127) do processo 0020437-45.2022.6.18.8000.

Documento assinado eletronicamente por **Aurélio Sodré Rocha**, **Analista Judiciário**, em 15/02/2023, às 11:29, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Rosemberg Maia Gomes**, **Coordenador de Desenvolvimento e Infraestrutura**, em 15/02/2023, às 11:33, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Carlos Alberto Ribeiro do Nascimento Junior**, **Chefe de Seção**, em 15/02/2023, às 11:35, 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 **1773866** e o código CRC **0D971E7B**.