TERMO DE REFERÊNCIA

1. OBJETO DA CONTRATAÇÃO

Esta licitação tem por objeto o Registro de Preços para contratação de solução de firewall com software de análise de logs, conexão 2FA para VPN e suporte/garantia de 60 meses. para segurança da informação de perímetro que possibilite a visibilidade e controle de tráfego e aplicações em camada 7, filtragem de conteúdo web, prevenção contra ataques e ameaças avançadas e modernas, filtro de dados, VPN e controle granular de banda de rede, compreendendo fornecimento de equipamentos e softwares integrados em forma de *appliance* conforme quantidades e exigências estabelecidas neste instrumento.

2. DESCRIÇÃO DA SOLUÇÃO DE TI

Devido as necessidades do Tribunal Regional Eleitoral do Acre em adquirir uma solução de firewall de próxima geração, as quantidades abaixo foram estimadas no estudo técnico preliminar para compor o projeto em sua totalidade.

Além disso, tal solução deve ser compatível com o software de gerenciamento, software este responsável por administrar as configurações e monitorar todos os equipamentos de segurança de perímetro de rede utilizados pelo Tribunal Regional Eleitoral do Acre.

2.1. Bens e serviços que compõem a solução

Item	Descrição	Quantidade	Unidade
1	Firewall de Borda	1	unidade
2	Firewall de Núcleo	2	unidade
3	Software de Gerenciamento e Relatório	3	unidade
4	Implantação com Hands On	2	serviço
5	Treinamento Oficial	4	pessoas

3. JUSTIFICATIVA PARA CONTRATAÇÃO

3.1. Contextualização e Justificativa da Contratação

Com o avanço constante da tecnologia cibernética, os hackers também avançam e desenvolvem novas técnicas de ataques maliciosos, seja em redes corporativas, de instituições públicas ou privadas, com o objetivo de sequestrar arquivos, dados pessoais ou informações corporativas importantes. Os criminosos virtuais podem ter diversos objetivos obscuros e atingiram tal ponto de ousadia que muitas vezes chegam a manter informações ou dados importantes criptografados (como reféns), até que a pessoa ou instituição pague um determinado valor como resgate (geralmente em *criptomoeda*) pela liberação destas informações ou até mesmo fazendo uso indevido das informações ilegalmente obtidas para vantagens próprias.

A constante modernização e ampliação dos aparatos de Tecnologia da Informação dentro de uma instituição, faz crescer a preocupação de todos sobre a proteção dos dados e da privacidade dos seus cidadãos. Além disso, algumas normativas governamentais como, por exemplo, a LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018), que entrou em vigor em agosto de 2020, que descreve aprimoramentos e regras de segurança no ambiente de TI visando a proteção e conservação dos dados e consequentemente da privacidade das pessoas, faz com que instituições públicas e privadas invistam cada vez mais em recursos tecnológicos para aprimorar sua segurança da informação e manter informações sensíveis protegidas.

O sistema de firewall funciona como um filtro eletrônico que examina o tráfego de dados da rede, sinalizando e protegendo as operações de transmissão ou recebimento de dados conforme regras, permissões e perfis de proteção que são realizadas dentro de suas configurações. Devido a essa característica, o adequado funcionamento do firewall apresenta-se como um elemento crucial para operação e segurança cibernética dos serviços tecnológicos no âmbito do campus Ceará Mirim.

O firewall de próxima geração tem a capacidade de prover visibilidade granular e analisar as ameaças de todo o tráfego de dados a nível de aplicação (camada 7), garantindo ainda mais segurança para a rede, com relação as ameaças que trafegam por estas aplicações.

Como o firewall é um equipamento de extrema importância para proteção e funcionamento da rede e que possibilita a conexão segura dos usuários remotos através de túneis VPN e que se inexistente ou indisponível por falha de hardware ou software, isso pode comprometer os serviços administrativos e operacionais do Campus. Portanto, dada a necessidade de modernização da solução de firewall, se faz necessário para este projeto a aquisição de solução de firewall de próxima geração. Além da premente necessidade de atualização por decurso tecnológico, outra urgência se mostra importante para a atualização do firewall de próxima geração existente no

O TRE-AC busca manter um sistema unificado de gestão centralizada das configurações e monitoramento dos equipamentos, o que traz maior agilidade e rapidez nas atividades do uso diário e administração da solução, geração de relatórios e nas atividades de investigação caso ocorra algum incidente de segurança.

3.2. Alinhamento aos Instrumentos de Planejamento Institucionais

Alinhamento Estratégico	
ID	**Objetivos Estratégicos**
	Fortalecimento da Estratégia Nacional de TIC e de Proteção de Dados.

Alinhamento ao PDTIC 2021 - 2023	

ID	Ação do PDTIC
PTS-13	Atualização de sistemas legados

Alinhamento a Estratégia Nacional de Cibersegurança da Justiça Eleitoral 2021 - 2024	
ID	**Descrição do Eixo Estruturante**
E3	Ferramentas Automatizadas

3.3. Estimativa da Demanda

Com base no Estudo Técnico Preliminar foram estimadas as seguintes quantidades a serem adquiridas pela instituição:

3.3.1. Secretaria do Tribunal Regional Eleitoral do Acre (Gerenciador), localizada no endereço Alameda Ministro Miguel Ferrante, 224 – Bairro Portal da Amazônia – CEP 69915-632 – Rio Branco - AC.

Item	Descrição	Quantidade	Unidade
1	Firewall de Borda	1	unidade
2	Firewall de Núcleo	2	unidade
3	Software de Gerenciamento e Relatório	3	unidade
4	Implantação com Hands On	2	serviço
5	Treinamento Oficial	4	pessoas

3.4. Parcelamento da Solução de TI

Os equipamentos e licenças que constituem a solução, aqui proposta, interagem entre si de forma a convergir para um sistema unificado, de modo que o fornecimento parcelado inviabilizaria a implantação de tecnologia capaz de atender as necessidades deste órgão.

A eventual divisão do objeto em grupos diversos poderia ocasionar uma situação onde um proponente “A”, por não conhecer a solução, não teria condições de fornecer eventual licenciamento correto para tal ou mesmo propor equipamentos compatíveis. Ante ao exposto, é evidente que o agrupamento do objeto, de maneira a compor uma solução unificada, é necessário a fim de evitar eventuais problemas de compatibilidade.

Ademais, lidar com um único fornecedor diminui o custo administrativo de gerenciamento de todo o processo de contratação. O aumento da eficiência administrativa do setor público passa pela otimização do gerenciamento de seus contratos de fornecimento. Essa eficiência administrativa também é de estatura constitucional e deve ser buscada pela administração pública.

Por fim, o agrupamento em lote, de todos os itens deste processo, visa garantir a otimização dos prazos de execução, viabilizando a sincronia nos fornecimentos e serviços de instalações, evitando assim que um fornecedor venha a prejudicar a execução de outro. Ainda, conforme disposto no inciso I, do artigo 15 da lei 8.666, de 21 de junho de 1993 (I - Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), estes equipamentos, por questões de compatibilidade, gerência, suporte e garantia, todos os itens deverão ser do mesmo fabricante.

3.5. Resultados e Benefícios a serem alcançados

Os benefícios a serem alcançados com a execução deste projeto são:

1. Adequação às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014)
2. Economia com gastos desnecessários provocados pelos resultados do risco de ataques a perímetro da rede institucional;
3. Padronização da tecnologia, conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I – Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), facilitando a administração da solução em casos específicos de suporte, assistência ou algo do gênero, não sendo necessário administrar vários pontos de contato para este fim;
4. Maior visibilidade do tráfego de rede e aplicações em camada 7, possibilitando a detecção e proteção em tempo real contra ameaças
5. Controle de utilização da rede, sendo possível a aplicação de filtros e bloqueios conforme perfil de usuários, controlando de forma granular a utilização dos recursos;
6. Maior visibilidade do tráfego de rede e aplicações em camada 7, possibilitando a detecção e proteção em tempo real contra ameaças;
7. Controle de utilização da rede, sendo possível a aplicação de filtros e bloqueios conforme perfil de usuários, controlando de forma granular a utilização dos recursos;
8. Proteção do ambiente de rede contra ameaças tipo worms, vírus, malwares entre outras pragas virtuais, atendendo às exigências do Marco Civil da Internet.
9. Geração de relatórios diversos para rápida análise de informações sobre tráfego,aplicações,ameaças, usuários,etc.
10. Criação de políticas de proteção da rede contra ataques de hackers através do bloqueio ou sancionamento de aplicações com o programa de compartilhamento de dados (P2P), fechamento de portas não utilizadas controlando a banda de internet afim de evitar abusos em sua utilização;
11. Criação de políticas e regras de uso de aplicações, acesso a certas categorias de URL,portas de serviços TCP e UDP(por grupo ou usuário);

Filtro de conteúdo URL, bloqueando acesso a sites indesejados de conteúdo ilícito e bloqueio de aplicações;

4. ESPECIFICAÇÃO DOS REQUISITOS DA CONTRATAÇÃO

Aquisição de solução de proteção de rede com características de Next Generation Firewall(NGFW) para segurança de informação perimetral que inclui filtro de pacote, controle de aplicação, administração de largura de banda (QoS), VPN IPSec e SSL, IPS, prevenção contra ameaças de vírus e spywares, Filtro de URL, bem como controle de transmissão de dados e acesso à internet compondo uma plataforma de segurança integrada e robusta.

4.1. Requisitos para os Firewalls (Itens 1 e 2)

4.1.1. Requisitos gerais comuns para os Firewalls (Itens 1 e 2)

1. A solução deve consistir de appliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW) tais como reconhecimento e controle de aplicações, identificação de usuários, prevenção contra ameaças de vírus, spywares e malwares desconhecidos (Zero Day), IPS, filtro de URL e recursos de VPN;
2. Possuir sistema de segurança com aplicação de filtros de pacotes baseados em regras, estados de conexão e inspeção profunda de pacotes
3. Deve permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound) através da classificação dos pacotes (shaping);
4. Emitir alarmes na console de administração integrada, alertas via correio eletrônico, syslog e traps SNMP;
5. Deve possuir MIB própria contemplando, no mínimo, indicadores de estado do hardware e interfaces WAN e performance do equipamento;
6. Possuir, no mínimo, suporte a SNMP v2 e v3;
7. Deve suportar, no próprio firewall, autenticação de usuários locais e integração com serviços de autenticação de diretório LDAP, Microsoft Active Directory e RADIUS;
8. Suportar e efetuar a captura de pacotes e exportação no formato PCAP.
9. Suportar tags de VLAN;
10. Todas as funcionalidades adquiridas de hardware e software devem operar conforme disposto neste Termo de Referência durante o prazo de garantia dos equipamentos, ou seja, o fornecedor deve garantir a atualização completa das funcionalidades no prazo referido, não sendo permitida a cobrança de quaisquer valores adicionais pelo uso dos hardwares e softwares para esse período. As funcionalidades deverão permanecer ativas, mesmo que não sejam atualizadas após o fim do prazo da garantia;
11. O fabricante deverá atualizar firmwares e softwares da solução para novas versões durante toda vigência da garantia;
12. O equipamento deve ser fornecido em hardware dedicado tipo appliance com sistema operacional otimizado, do mesmo fabricante, para o uso como firewall corporativo multifuncional.
13. O equipamento deve possuir 1 (uma) porta de console para configuração e gerenciamento por interface de linha de comando (CLI).
14. Fonte de alimentação com operação automática entre 110 e 220V;
15. Prover servidor DHCP interno suportando no mínimo um escopo por interface e a funcionalidade de DHCP Relay;
16. Prover mecanismo de conversão de endereços (NAT), de forma a possibilitar que uma rede com endereços reservados acesse a Internet a partir de um único endereço IP e possibilitar também um mapeamento 1-1 de forma a permitir com que servidores internos com endereços reservados sejam acessados externamente através de endereços válidos;
17. Possuir suporte a redes IPv6 e IPv4;
18. Possuir o gerenciamento de tráfego de entrada e saída por serviços, endereços IP e regra de firewall, permitindo definir banda mínima garantida e máxima permitida;
19. Implementar os serviços de Provedor VPN baseado no protocolo IPsec, com certificação digital;
20. Todos os equipamentos, produtos, peças ou software ofertados deverão ser novos e de primeiro uso e não constar, no momento da apresentação da proposta, em listas de end-of-sale, end-of-support ou end-of-life do fabricante, ou seja, não deverão ter previsão de descontinuidade de serviço, suporte ou vida, devendo estar em linha de produção do fabricante e cobertos por contratos de suporte e atualização de versão do fabricante pelo período mínimo de 60 (sessenta) meses;
21. A solução de firewall deve possuir garantia pelo período de, no mínimo, 60 (sessenta) meses, compreendendo a reposição de peças/equipamentos, atualizações do sistema operacional do equipamento e demais software e das assinaturas de proteção da solução.
22. Não serão permitidas soluções baseadas em redirecionamento de tráfego para dispositivos externos ao appliance para análise de arquivos ou pacotes.
23. O equipamento fornecido deve ser próprio para montagem em rack 19”, incluindo kit para adaptação, se necessário, e cabos de alimentação;
24. Deve possuir o recurso de agregação de links conforme padrão IEEE 802.3ad (LACP) permitindo o agrupamento de interfaces físicas de rede em um link agrupado virtualmente (LAG – Link Aggregation Group);
25. Suportar, no mínimo, os protocolos de roteamento dinâmico OSPF v3 e BGP, bem como as funcionalidades de roteamento estático e roteamento policy-based;
26. Deve permitir o envio de logs para sistemas de monitoração externos utilizando o padrão syslog, bem como o envio de forma segura através do protocolo SSL/TLS;
27. Deve possuir o recurso de alta disponibilidade e permitir a configuração nos modos ativo/passivo e ativo/ativo;
28. Deve implementar controle por políticas/regras de firewall capaz de permitir ou bloquear o tráfego de rede por porta e protocolo, por aplicações, por grupos estáticos de aplicações, por grupos dinâmicos de aplicações baseados em características e comportamento das aplicações, por usuários e grupos de usuários, por endereços IP e faixas de endereços IP e por país de origem e destino do tráfego;
29. Deve possuir a capacidade para realizar a decriptografia do tráfego SSL e SSH permitindo o controle e inspeção tanto do tráfego de entrada quanto de saída. A decriptografia deve ser realizada com base em políticas/regras de acordo com a origem e destino do tráfego;
30. Deve possuir recurso de QoS – Quality of Service com suporte a DSCP – Differentiated Services Code Point. Deve permitir também definir, baseado em políticas/regras, a prioridade e o limite máximo de largura de banda de um determinado tipo de tráfego. As definições de prioridade e limite de largura de banda devem ser baseadas no endereço IP de origem e destino, no usuário e na aplicação;
31. A solução de firewall deve possuir integração com LDAP, MS Active Directoy e RADIUS para identificação dos usuários e grupos da rede para uso nas políticas/regras baseadas por usuários e grupo de usuários;
32. Deve ser possível criar perfis de acesso à interface de gerenciamento com permissões granulares como acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações entre outros;
33. Deve permitir realizar o backup das configurações do equipamento e a restauração da configuração salva através de interface de gerenciamento;
34. Por cada equipamento que compõe a solução de segurança, entende-se o hardware e as licenças de softwares necessárias para o seu funcionamento;
35. Deve possuir a capacidade de reconhecer aplicações diferentes tais como redes sociais, compartilhamento de arquivos, e-mail, atualização de softwares, acesso remoto, VoIP, áudio e vídeo, peer-to-peer, sistemas de mensagem instantânea, etc, sendo esta uma lista não exaustiva;
36. O reconhecimento da aplicação se dará, independentemente de porta e protocolo, através de, no mínimo, os seguintes métodos: baseado na assinatura da aplicação conhecida pelo fabricante da solução de firewall, através da decodificação de protocolos para detectar aplicações encapsuladas dentro do protocolo e identificação através de análise heurística a fim de detectar aplicações através de análise comportamental do tráfego analisado;
37. Deve permitir a diferenciação e controle de partes da aplicação como, por exemplo, em uma aplicação de mensagem instantânea permitir a troca de mensagens de texto e bloquear a transferência de arquivos por dentro da aplicação;
38. Deve permitir bloquear sessões TCP que utilizarem variações do three-way handshake como four-way e o five-way split handshake, prevenindo assim possíveis tráfegos maliciosos;
39. Deve permitir bloquear conexões que contenham dados no payload dos pacotes TCP SYN e TCP SYN-ACK durante o three-way handshake;
40. A solução de firewall deve possuir funcionalidades de IPS, antivírus e anti-spyware que permita o bloqueio de vulnerabilidades e exploits conhecidos e proteção contra vírus e spywares baseado em assinaturas de ameaças conhecidas;

41. Deve ser possível a criação de assinaturas customizadas de ameaças;
42. Deve permitir realizar o bloqueio de vírus realizando a inspeção em, no mínimo, os protocolos HTTP, FTP, SMB, SMTP e POP3. Será permitido o uso de appliance externo para o bloqueio de vírus caso a solução de firewall ofertada não realize nativamente a inspeção em algum dos protocolos solicitados;
43. Deve possuir a capacidade de detectar e prevenir ameaças em tráfego HTTP/2;
44. Deve possuir proteção contra ataques de negação de serviço (DoS) capaz de impedir ataques de SYN Flood, ICMP Flood, UDP Flood, etc e deve também bloquear port scans, bloquear ataques de buffer overflow e identificar e bloquear comunicação com botnets;
45. Para cada ameaça detectada pela solução deve ser realizado o registro nos logs do sistema das informações de data e hora, tipo da ameaça, origem e destino da comunicação e a ação tomada (se permitiu ou bloqueou o tráfego);
46. A solução de firewall deve possuir funcionalidade de filtro URL que permita a criação de políticas/regras para controle do acesso a websites baseado em categorias de URL devendo o fabricante da solução disponibilizar a base de dados de URL categorizadas para consulta por parte da solução. As políticas/regras que permitem ou bloqueiam o acesso a determinada categoria de URL devem ser com base no usuário e grupos de usuários e por endereços IP e faixas de endereços IP;
47. Deve permitir a criação de categoria de URL customizada permitindo inserir uma lista de URLs específicas;
48. Deve permitir a customização da página de bloqueio exibida ao usuário quando o mesmo tentar realizar um acesso a um website pertencente a uma categoria de URLs bloqueada;
49. A solução de firewall deve possuir recurso de portal de autenticação prévia (Captive Portal) para identificação dos usuários que realizam o acesso à internet, sem a necessidade de instalação de software cliente ou agente no computador. O portal de autenticação deve ser exibido antes de o usuário iniciar a navegação pela internet;
50. A solução de firewall deve possuir o recurso de VPN – Virtual Private Network dos tipos site-to-site e client-to-site e suportar IPSEc – Internet Protocol Security e SSL – Secure Sockets Layer;
51. O recurso de VPN SSL deve permitir que o usuário remoto se conecte através de um software cliente de VPN instalado no sistema operacional do equipamento do usuário sendo possível a atribuição de endereços IP fixos e atribuição de DNS ao mesmo;
52. Deve suportar a autenticação dos usuários remotos que se conectam à VPN via LDAP, MS Active Directory, RADIUS e através de base de usuários local no equipamento da solução de firewall. Deve suportar também a autenticação via certificado;
53. Deve ser disponibilizado o software cliente de VPN do mesmo fabricante da solução de firewall ofertada compatível para instalação em computadores com sistema operacional, MS Windows 10, MacOS e Linux e para instalação em dispositivos móveis Android e IOS;
54. A solução de firewall deve possuir console de gerenciamento do equipamento acessada através de interface gráfica web permitindo realizar as configurações da solução como criar e administrar as políticas/regras de firewall e controle de aplicações, criar e administrar as políticas de IPS, antivírus e anti-spyware, criar e administrar as políticas de filtro URL, monitorar e investigar os registros de logs de eventos e demais configurações;
55. Deve ser possível através de interface de gerenciamento do equipamento a geração de relatórios tais como um resumo gráfico das aplicações utilizadas e ameaças vistas, principais aplicações por utilização de largura de banda, atividades de um usuário ou grupo de usuário específicos incluindo aplicações e URLs acessadas e permitir a criação de relatórios personalizados;
56. Deve ser exibida na interface gráfica de gerenciamento do equipamento informações em tempo real, atualizadas de forma automática a cada 1 (um) minuto, as principais aplicações acessadas, o risco das principais aplicações, número de sessões simultâneas, status das interfaces de rede e uso de CPU;
57. Deve permitir configurar o agendamento das políticas/regras de firewall para habilitar ou desabilitar tais políticas/regras em horários pré-definidos;
58. Garantia e Suporte
    1. Deve possuir garantia do fabricante com validade mínima de 60 (sessenta) meses;
    2. Durante o prazo de garantia, deve ser possível realizar a atualização de sistema operacional dos equipamentos para obter novas funcionalidades e correção de bugs;
    3. Em caso de defeitos de fabricação, a garantia deve incluir envio de peças ou equipamentos de reposição, obedecendo a modalidade NBD (Next Business Day);
    4. Os chamados poderão ser abertos diretamente com o fabricante;
    5. A empresa contratada deverá disponibilizar, cumulativamente, estrutura de suporte técnico por meio de atendimento telefônico ou website ou e-mail;
    6. A contratada deverá disponibilizar um portal web com disponibilidade de 24 horas por dia, 7 dias por semana, com sistema de help-desk para abertura de chamados de suporte técnico;
    7. A equipe técnica da contratante poderá abrir, gerenciar status e conferir todo o histórico de chamados de suporte técnico, mediante login e senha de acesso ao sistema;
    8. Todo o chamado aberto deverá ter sua resolução técnica registrada no sistema web de help-desk;
    9. A contratada deve indicar, por ocasião do início dos trabalhos, os procedimentos para abertura de suporte técnico;
    10. As horas de atendimento pelo suporte cumulativo da contratada serão realizadas normalmente em horário comercial, no período compreendido entre 08:00 e 18:00h, em dias de semana (segunda à sexta).
59. Condições de Entrega
    1. Os equipamentos deverão ser entregues na unidade responsável pelo recebimento no TRE-AC na Seção de Patrimônio e Almoxarifado - SEMAP, localizada no local indicado no sub tópico **3.3.1**, de segunda-feira a sexta-feira no horário estipulado no referido anexo, ou em outro horário previamente agendado com a gestão da contratação, no prazo máximo de 90 (noventa) dias corridos, contados a partir da publicação do extrato do contrato.
    2. Todos os produtos fornecidos deverão ser novos, em linha de produção e de primeiro uso, Não serão aceitos equipamentos remanufaturados, NFR (Not For Resale) ou de demonstração. Os equipamentos deverão ser entregues nas caixas lacradas pelo fabricante, não sendo aceitos equipamentos com caixas violadas;
    3. A entrega deverá ser previamente agendada junto ao Tribunal Regional Eleitoral;
    4. Os equipamentos deverão atender rigorosamente a todas as especificações técnicas exigidas, inclusive no tocante a marcas, modelos dos componentes e módulos internos e externos, conforme cotados pela contratada.
    5. A unidade responsável pelo recebimento no TRE atestará no verso da Nota Fiscal o recebimento provisório dos equipamentos e a encaminhará ao Gestor da Contratação para aceite definitivo.
60. Condições de Aceite
    1. O aceite do bem somente será dado após comprovação da entrega e o efetivo cumprimento de todas as exigências da presente especificação técnica;
    2. Será consultado diretamente no site do fabricante do equipamento manuais e toda documentação pública disponível para comprovação do pleno atendimento aos requisitos deste edital. Em caso de dúvida ou divergência na comprovação da especificação técnica, este órgão poderá solicitar amostra do equipamento ofertado, sem ônus ao processo, para comprovação técnica de funcionalidades. Esta amostra deverá ocorrer em até 15 (quinze) dias úteis após a solicitação deste órgão. Para a amostra, a empresa deverá apresentar o mesmo modelo do equipamento ofertado no certame, com técnico certificado na solução para configuração e comprovação dos itens pendentes,

nas dependências deste órgão (conforme itens 1.1.1 e 1.1.2, TC-006.806/2006-4, Acórdão nº 838/2006-TCU-2ª Câmara);

4.1.2 Requisitos Específicos de Firewall - Item 1 (Firewall de Borda)

Requisitos de desempenho mínimo:

Especificação mínima	**Valor**
Quantidade de interfaces padrão 1 Gbps	12
Quantidade de interfaces padrão 10 Gbps	3
Conexões simultâneas	900.000 (novecentos mil)
Novas conexões por segundo	22.000 (vinte e dois mil)
Clientes VPN SSL simultâneos licenciados com solução de 2FA completamente habilitada e totalmente licenciada	500 (quinhentos)
Capacidade de usuários VPN SSL simultâneos	500 (quinhentos)
Taxa de transferência throughput ([1])	2.3 Gbps
Storage Mínimo	128 GB

4.1.3 Requisitos Específicos de Firewall - Item 2 (Firewall de Núcleo)

Requisitos de desempenho mínimo:

Especificação mínima	**Valor**
Quantidade de interfaces padrão 1 Gbps	8
Quantidade de interfaces padrão 10 Gbps	2
Conexões simultâneas	2.000.000(dois milhões)
Novas conexões por segundo	115.000 (cento e quinze mil)
Clientes VPN SSL simultâneos licenciados com solução de 2FA completamente habilitada e totalmente licenciada	2
Taxa de transferência throughput ([2])	3.6 Gbps
Storage Mínimo	128 GB

4.2. Requisitos Específicos - Software de Gerenciamento e Relatório (Item 3)

1. Deve prover gestão centralizada de todos os dispositivos do lote;
2. Deve estar licenciado, no mínimo, para o quantitativo de licenças solicitadas pelo CONTRATANTE. O item será por unidade licenciada;
3. Deve ser homologado e totalmente compatível com os Firewalls especificados neste Termo de Referência para permitir o gerenciamento centralizado e armazenamento de logs dos mesmos, possuindo escalabilidade para acréscimo de no mínimo 154 firewalls;
4. Deve ser do tipo Appliance Físico, Appliance Virtual ou solução de software baseada em máquina virtual (VM). Caso seja entregue em appliance físico ele deve ser compatível com rack 19 polegadas e possuir todos os acessórios necessários para sua instalação. Caso seja baseada em Máquina Virtual (VM), a PROPONENTE deverá indicar em sua proposta qual a necessidade de hardware a ser disponibilizada para a respectiva instalação;
5. Caso seja em VM, deve ser compatível com VMware ESX(i);
6. Deve suportar operação em alta disponibilidade (HA) sincronizando as mudanças na base de dados entre as estações de gerência;
7. Na data da proposta, nenhum dos softwares ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;
8. Permitir acesso concorrente de administradores;
9. Bloqueio de alterações, no caso de acesso simultâneo de dois ou mais administradores;
10. Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;
11. Gerar alertas automáticos via Email;
12. Gerar alertas automáticos via SNMP;
13. Deve suportar backup/restore de todas as configurações da solução de gerência, permitindo ao administrador agendar backups da configuração em um determinado dia e hora;
14. As alterações realizadas em um servidor de gerência deverão ser automaticamente replicadas para o servidor redundante;
15. Deve suportar sincronização do relógio interno via protocolo NTP;
16. Deve registrar as ações efetuadas por quaisquer usuários;
17. Devem ser fornecidos manuais de instalação, configuração e operação de toda a solução, na língua portuguesa ou inglesa, com apresentação de boa qualidade, podendo ser disponibilizados na internet;
18. Suportar SNMP versão 2 e versão 3 nos equipamentos de gerência;

19. O gerenciamento deve possibilitar a criação e administração de políticas de firewall e controle de aplicação;
20. O gerenciamento deve possibilitar a criação e administração de políticas de IPS, Antivírus e Anti-Spyware;
21. O gerenciamento deve possibilitar a criação e administração de políticas de Filtro de URL;
22. Permitir criação de regras que fiquem ativas em horário definido;
23. Deve permitir que todos os firewalls sejam controlados de forma centralizada utilizando apenas um servidor de gerência;
24. O servidor de gerência deve ser hospedado em um equipamento independente, não exercendo funções de firewall;
25. A solução deve incluir uma ferramenta para gerenciar centralmente as licenças de todos os appliances controlados pela estação de gerenciamento, permitindo ao administrador atualizar licenças nos appliances através dessa ferramenta;
26. A solução deve possibilitar a distribuição e instalação remota, de maneira centralizada, de novas versões de software dos appliances;
27. Permitir visualizar, a partir da estação de gerência centralizada, informações detalhadas dos dispositivos gerenciados;
28. Deve permitir a criação de objetos e políticas compartilhadas;
29. Deve mostrar os status dos equipamentos de firewalls em alta disponibilidade a partir da solução de gerenciamento centralizado;
30. Deve prover console unificada e centralizada;
31. Deve auxiliar na solução e identificação de ameaças;
32. Deve ser do mesmo fabricante dos demais itens do lote;
33. A solução de gerenciamento centralizado e relatório deve possibilitar a coleta de estáticas de todo o tráfego que passar pelos equipamentos de firewall gerenciados pela solução, além de consolidar os registros de eventos (logs) e relatórios de todos os equipamentos que compõem a solução de proteção de rede;
34. Deve consolidar logs e relatórios de todos os equipamentos de firewall gerenciados;
35. A solução deve possuir garantia pelo período de, no mínimo, 60 (sessenta) meses, compreendendo a atualização do software para obter novas funcionalidades e correções de bugs.
36. Caso haja soluções específicas para gerenciamento e relatório, a CONTRATADA deverá prover a quantidade de licenças para ambas as soluções.

4.3. Requisitos Específicos – Implantação Com Hands On (Item 4)

1. A instalação e configuração compreenderá apenas os firewalls de borda e núcleo, sendo uma unidade deste item aplicada à implantação de até dois equipamentos de borda ou até dois equipamentos de núcleo visando a implantação de alta disponibilidade;
2. Os serviços de instalação e configuração, compreendem, entre outros, os seguintes procedimentos:
    1. Análise da topologia e arquitetura da rede, considerando os roteadores, servidores de aplicação e firewall já existentes e instalados;
    2. Análise do acesso Internet, sites remotos, serviços de rede oferecidos aos funcionários e aos usuários externos;
    3. Regras de Firewall existentes e aplicáveis à solução ofertada dada a colocação desta na Rede deste parque;
    4. Análise do posicionamento de qualquer outro equipamento ou sistema relevante na segurança de qualquer perímetro protegido pela solução;
    5. Apresentação em até 5 dias corridos do plano de implantação com o descritivo de todos os serviços a serem executados e topologia física e lógica a ser implementada;
    6. A realização dos ajustes de hardware e software necessários ao funcionamento dos equipamentos.
    7. Aplicação de todas as atualizações de firmware ou qualquer outro software componente da solução, para a versão mais atualizada disponível ou a última compatível com as demais soluções deste lote e considerada estável.
    8. Configuração do sistema de Firewall, VPN, IPS, Filtro URL, Antivírus e Anti-Malware de acordo com as exigências levantadas com as devidas atualizações necessárias;
    9. Instalação de Sistema de Gerência Centralizada em Appliance Físico, Appliance Virtual ou solução baseada em VM (máquina virtual), de acordo com a oferta da CONTRATADA. O mesmo será considerado entregue, quando for instalado e configurado, com todas as atualizações, configurações e licenças. Deverão ser adicionados a este todos os firewalls instalados contemplados na solução adquirida, e que deverão estar sendo monitorados e gerenciados por este Sistema de Gerência Centralizada;
    10. Habilitação das licenças que porventura sejam adquiridas e recursos do equipamento que serão utilizados pela solução.
    11. Inclusão de políticas de segurança encaminhadas pelo respectivo TRE, pré-existentes em seu ambiente, para os novos equipamentos;
3. A CONTRATADA deverá, ao final dos trabalhos, fornecer a entrega da documentação técnica completa da solução referente aos procedimentos de instalação e configuração, bem como fornecer um repasse sobre a solução e as configurações realizadas.
    1. Deve haver geração de relatório e entrega da documentação da instalação com as configurações efetuadas e as decisões tomadas, diagramas e topologias em formato legível e tecnicamente fundamentado;
    2. A CONTRATADA deverá ministrar treinamento do tipo “Hands On” sobre a solução de Firewall adquirida, incluindo instalação, configuração básica e avançada, troubleshoot, monitoramento e gerenciamento;
    3. A carga horária mínima será de 10 horas;
    4. O repasse deverá ter caráter prático e se baseará no sistema Firewall efetivamente instalado na CONTRATANTE;
4. É de responsabilidade da CONTRATADA designar um profissional certificado pelo Fabricante, fornecer todo material audiovisual, didático e, caso necessário, outros equipamentos eletrônicos para a realização dos treinamentos, além de impressos.
5. Todos os demais custos, ônus, obrigações e encargos para o treinamento devem ser arcados pela CONTRATADA.
6. O fiscal técnico acompanhará os trabalhos e aprovará a documentação técnica entregue em até 10 (dez) dias corridos.

4.4. Requisitos Específicos – Treinamento (Item 5)

1. A contratada deverá disponibilizar um voucher individual para participação no treinamento oficial do fabricante dos Firewalls ofertado;
2. O treinamento deve ser ministrado abrangendo teoria e prática de configuração e administração de solução de firewall de próxima geração, bem como assuntos teóricos relacionados;
3. Deve conter, no mínimo, a seguinte ementa:
    1. Arquitetura e Plataforma;
    2. Configuração da Solução;
    3. Políticas de Segurança e NAT;
    4. Políticas de segurança baseada em aplicação;
    5. Identificação de Aplicações;
    6. Identificação de Usuário;
    7. Bloqueio de ameaças;

8. Bloqueio de ameaças desconhecidas;
9. Bloqueio de ameaças em de tráfego criptografado;
10. Análise das informações de tráfego e ameaças detectadas;
11. Demais assuntos pertinentes a solução;

4. A duração do curso será de no mínimo 5 dias em horário comercial;
5. Deve ser emitido um único certificado de conclusão cobrindo todo o curso para o participante;
6. O treinamento deverá ser ministrado pelo próprio fabricante ou por um parceiro nacional, capacitado, certificado e autorizado pelo fabricante a ministrar treinamentos oficiais;
7. O treinamento deve estar disponível na modalidade presencial nas instalações do fabricante ou da autorizada ou ministrado de forma remota;
8. O fabricante ou autorizada fornecerá os materiais didáticos para ministrar o curso;
9. Não será necessário considerar na proposta os custos de deslocamento, hospedagem e alimentação dos alunos. Esses custos serão de responsabilidade da Contratante;

5. RESPONSABILIDADES

5.1. Deveres e responsabilidades da CONTRATANTE

1. Efetuar o pagamento nas condições e preços ora pactuados, desde que não haja qualquer óbice legal nem fato impeditivo provocado pela CONTRATADA;
2. Prover todas as condições necessárias para o desenvolvimento das atividades contratadas;
3. Comunicar à CONTRATADA as alterações que entender necessárias à realização do objeto da contratação, nos termos da proposta comercial;
4. Notificar a CONTRATADA, via e-mail, salvo a abertura de chamados técnicos, sobre a ocorrência de eventuais falhas no curso da execução dos serviços por meio de seus Fiscais ou Gestores;
5. Acompanhar e fiscalizar a execução do contrato por meio de servidor da Coordenadoria de Infraestrutura especialmente designado pela administração, nos termos do art. 67 da Lei 8.666/93, exigindo seu fiel e total cumprimento;
6. Responsabilizar-se pela comunicação, em tempo hábil, dos serviços a serem executados;
7. Arcar com as despesas com a publicação do extrato do contrato no Diário Oficial da União, que será providenciada pela administração até o 5º (quinto) dia útil do mês subsequente ao de sua assinatura, para ocorrer no prazo máximo de 20 (vinte) dias daquela data, nos termos do parágrafo único do art. 61 da Lei 8.666/93;
8. Efetuar toda a comunicação originada pelo contratante através de mensagem de correio eletrônico, salvo a abertura de chamados técnicos, endereçada ao representante da CONTRATADA;
9. Realizar, através da gestão contratual, todo o acompanhamento referente à utilização dos serviços contratados.

5.2. Deveres e responsabilidades da CONTRATADA

1. Cumprir fielmente as obrigações assumidas, conforme as especificações constantes neste Termo de Referência, utilizando-se de todos os recursos materiais e humanos necessários para entregar os produtos licitados no prazo;
2. Arcar com todas as despesas, diretas ou indiretas, decorrentes do cumprimento das obrigações assumidas, responsabilizando-se pelos danos causados diretamente à administração ou a terceiros, decorrentes de sua culpa ou dolo, sem qualquer ônus ao TRE-AC;
3. Ser responsável pelos encargos trabalhistas, previdenciários, fiscais e comerciais resultantes da execução contratual. A inadimplência da CONTRATADA, com referência aos encargos estabelecidos neste subitem não transfere a responsabilidade por seu pagamento à administração do TRE-AC, nem poderá onerar o objeto da licitação, razão pela qual a CONTRATADA renuncia expressamente a qualquer vínculo de solidariedade, ativa ou passiva, com o TRE-AC;
4. Prestar todos os esclarecimentos que forem solicitados pelo TRE-AC, credenciando um representante para prestar os devidos esclarecimentos e atender às reclamações que porventura surgirem durante a execução do objeto;
5. Quando, por problemas técnicos, os prazos pactuados não puderem ser cumpridos, a CONTRATADA deverá comunicar por escrito ao TRE-AC até 2 (dois) dias úteis anteriores ao término do prazo, cabendo ao gestor do contrato aceitar ou rejeitar as justificativas;
6. A CONTRATADA é obrigada a reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou de materiais empregados;
7. Não transferir a outrem, no todo ou em parte, o objeto da presente contratação, sem prévia e expressa anuência do TRE-AC;
8. Informar qualquer alteração necessária à consolidação dos ajustes decorrentes da execução do objeto, tais como: mudança de endereços, razão social, telefone, fax, dissolução da sociedade, falência e outros;
9. Comunicar imediatamente ao gestor do contrato, qualquer anormalidade verificada, inclusive de ordem funcional, para que sejam adotadas as providências de regularização necessárias, em qualquer tempo até o final da garantia;
10. Responder, para cada um dos itens do contrato por todas e quaisquer obrigações relativas a direitos de marcas e patentes, ficando esclarecido que a CONTRATANTE não aceitará qualquer imputação nesse sentido; além de atender a todos os encargos, inclusive os de natureza tributária, incidentes sobre o funcionamento do objeto (ISS, PIS e COFINS), cabendo-lhe, também, a responsabilidade total e exclusiva, pela reparação de quaisquer danos diretos causados a pessoas e a bens ou serviços do CONTRATANTE ou de terceiros, ou em virtude de manuseio ou utilização dos produtos por ela fornecidos;
11. Garantir, na atualização dos softwares relativos ao contrato de suporte, enquanto vigente a contratação, o fornecimento de upgrades para versões mais recentes, bem como releases e patches das licenças de uso dos softwares, não implicando em custos adicionais para a contratação;
12. Garantir acesso aos canais de suporte técnico no regime de 24x7 - 24 horas, 7 dias na semana, através de número de telefone de discagem gratuita (0800) e/ou internet, para abertura de chamados técnicos, objetivando a resolução de problemas e dúvidas quanto ao funcionamento dos softwares, bem como permitir a utilização de estrutura de pesquisa em base de conhecimento de solução de problemas e documentos técnicos, todos de propriedade da CONTRATADA;
13. Manter confidencialidade e, em nenhum momento, divulgar a terceiros, sem a ciência e o consentimento do CONTRATANTE, documentos, imagens/fotos, dados ou outra informação que tiver sido direta ou indiretamente proporcionada pelo CONTRATANTE, antes, durante ou depois de encerrada a vigência do contrato, nos termos da política de suporte técnico da CONTRATADA;
14. Obedecer as normas de segurança da informação existentes na Justiça Eleitoral e também as normas/regras específicas do TRE responsável pela aquisição.

6. MODELO DE EXECUÇÃO DO CONTRATO

6.1. Dinâmica (Art. 18, § 3º, III, a, 2)

1. Após o início da vigência da ata de registro de preços, a SCSEG (Seção de Cibersegurança) solicitará à Coordenadoria de Material e Patrimônio (COMAP), através de meio eletrônico, o pedido de entrega do quantitativo de itens necessários obedecendo ao mínimo e máximo estipulados neste termo de referência.
2. O acompanhamento do pedido de entrega dos equipamentos (ITENS 1 e 2) será realizado pela COMAP.

3. Após a entrega do(s) equipamento(s) solicitados, a COMAP, ou setor responsável, informará ao gestor da contratação, por mensagem eletrônica, do aceite provisório do objeto e encaminhará o objeto e a respectiva nota fiscal para aceite definitivo.
4. O recebimento e aceites técnicos, provisório e definitivo, serão realizados conforme descrito no item 6.5 deste termo de referência pela equipe de gestão da contratação (gestor do contrato e fiscal técnico).
5. Os itens relativos a serviços (ITENS 3, 4 e 5) serão solicitados e acompanhados pela gestão da contratação.
6. Após a entrega do(s) serviço(s) solicitados, o fiscal técnico da equipe de contratação em cada TRE, efetuará o aceite provisório do objeto e encaminhará a respectiva nota fiscal para aceite definitivo pelo gestor da contratação, conforme item 6.5.
7. Após o aceite definitivo, o gestor da contratação atestará a nota fiscal e a encaminhará de volta para o setor responsável que procederá aos trâmites institucionais de envio para pagamento.
8. Em caso de falhas dentro do período de garantia, deverão ser seguidos os procedimentos de garantia definidos neste termo de referência.

6.2. Instrumentos Formais (Art. 18, § 3º, III, a, 3)

1. A solicitação de fornecimento dos bens e/ou da prestação de serviços será formalizada através de meio eletrônico, conforme registrado no tópico 6.1 deste documento.
2. A contratação será formalizada através de instrumento contratual entre as partes.
3. A vigência do contrato será a partir da publicação do seu extrato no diário oficial e terá duração de 60 (sessenta) meses para todos os itens relativos a materiais (FIREWALLS, SOFTWARES e FERRAMENTA DE ANÁLISE DE LOG).
4. A vigência do contrato para os itens de serviços (IMPLANTAÇÃO E TREINAMENTO) contará a partir da publicação do seu extrato no diário oficial e terá duração de 06 (seis) meses.

6.3. Acompanhamento (Art. 18, § 3º, III, a, 4)

A gestão do contrato verificará, durante o período de vigência contratual, o cumprimento dos requisitos descritos no tópico 3 deste termo de referência, podendo solicitar a aplicação de sanção em caso de descumprimento.

6.4. Comunicação (Art. 18, § 3º, III, a, 5)

A comunicação ocorrerá sempre através de mensagem de correio eletrônico endereçada ao representante da Contratada.

6.5. Recebimento (Art. 18, § 3º, III, a, 6)

6.5.1. Para os itens 1 e 2:

6.5.1.1 Entrega dos equipamentos

Os equipamentos deverão ser entregues conforme descreve o item 59 do tópico 4.1.1.

6.5.1.2 Aceite dos Equipamentos

Os Equipamentos serão recebidos:

a) provisoriamente pela SEMAP, para que seja feita a verificação gerais no recebimento.

b) definitivamente, após avaliação e homologação pelo fiscal técnico da Contratação conforme as especificações, da seguinte forma:

b.1) O exame para comprovação das características técnicas consistirá em avaliações e testes não-destrutivos, por amostragem realizados em duas etapas:

- Primeira etapa: inspeção visual de todos os equipamentos entregues;

- Segunda etapa: testes funcionais de configuração e desempenho, em, no mínimo, 10% (dez por cento) e não menos do que 01 (um) dos equipamentos recebidos.

O Fiscal Técnico poderá, a seu critério, executar os testes nos demais equipamentos, dentro de um critério de razoabilidade, podendo chegar a 100% dos quantitativos, mas dentro de um prazo máximo de 10 (dez) dias corridos a partir do recebimento provisório.

b.2) As especificações serão avaliadas também por meio de documentos técnicos que acompanham os equipamentos, informações fornecidas pela Contratada e disponível no sítio do fabricante;

b.3) O fiscal técnico deverá, após a comprovação do perfeito funcionamento dos equipamentos e adequação às especificações técnicas, emitir e assinar o Laudo de Inspeção Técnica TRE;

b.4) O produto será rejeitado no caso de incompatibilidade com as especificações previstas na proposta ou quando inadequado à sua utilização.

b.5) O prazo para emissão do Laudo de Inspeção Técnica TRE será de até 10 (dez) dias corridos (após o recebimento provisório), quando deverá se manifestar, aceitando ou recusando o item objeto do fornecimento.

b.6) O objeto que estiver em desacordo com as especificações do edital terá seu recebimento recusado, devendo o fornecedor, dentro do prazo de 20 (vinte) dias corridos após a comunicação pela contratante, substituir o produto adequadamente, sujeitando-se às sanções previstas neste Termo de Referência.

b.7) Após a inspeção técnica nos equipamentos e verificando que estes estão em perfeitas condições de funcionamento, o Fiscal Técnico deverá encaminhar o Laudo de Inspeção Técnica TRE ao Gestor da Contratação para que seja emitido o aceite definitivo;

b.8) Após o recebimento do Laudo de Inspeção Técnica, o Gestor da Contratação emitirá, em até 5 (cinco) dias corridos o aceite definitivo, que por sua vez será item necessário para a liberação da nota fiscal para pagamento;

b.9) O recebimento definitivo não exime o fornecedor de responder pelos vícios aparentes e ocultos segundo as disposições deste termo e as normas de proteção ao consumidor.

6.5.2. Para o item 3 (software de gerenciamento/ de gerenciamento e relatório):

1. Após o envio de Nota de Empenho, o Gestor da Contratação encaminhará uma solicitação por mensagem eletrônica, solicitando o envio das referidas licenças adquiridas;
    - O prazo de entrega das licenças deve ser de, no máximo, 90 (noventa) dias corridos;
2. O fiscal técnico realizará o aceite provisório verificando se as licenças correspondem às indicadas na proposta em até 10 (dez) dias corridos, quando deverá se manifestar através de Laudo de Inspeção Técnica TRE, aceitando ou recusando o item objeto do fornecimento.
3. O objeto que estiver em desacordo com as especificações do edital terá seu recebimento recusado, devendo o fornecedor, dentro do prazo de 10 (dez) dias corridos após a comunicação pela contratante, substituir o produto adequadamente, sujeitando-se às sanções previstas neste Termo de Referência.
4. Após a inspeção técnica nas licenças e verificando que estas estão em perfeitas condições de funcionamento, o Fiscal Técnico deverá encaminhar o Laudo de Inspeção Técnica TRE ao Gestor da Contratação para que seja emitido o aceite definitivo;
5. Após o recebimento do Laudo de Inspeção Técnica, o Gestor da Contratação emitirá, em até 5 (cinco) dias corridos o aceite definitivo, que por sua vez será item necessário para a liberação da nota fiscal para pagamento;
6. O recebimento definitivo não exime o fornecedor de responder pelos vícios aparentes e ocultos segundo as disposições deste termo e as normas de proteção ao consumidor.

6.5.3. Para o item 4 (implantação com hands on):

1. Após o envio de Nota de Empenho, o Gestor da Contratação encaminhará uma solicitação por mensagem eletrônica, agendando a data

reservada para a execução dos serviços de implantação que deve ser finalizado em no máximo 30 (trinta) dias corridos a partir do aceite definitivo dos equipamentos adquiridos;

2. A instalação e configuração compreenderá apenas os firewalls de borda e núcleo, sendo uma unidade deste item aplicada à implantação de até dois equipamentos de borda ou até dois equipamentos de núcleo visando a implantação de alta disponibilidade;
3. A implantação hands on não será aplicada para os firewalls de cartório;
4. A instalação e configuração compreenderá:
    - A realização dos ajustes de hardware e software necessários ao funcionamento dos equipamentos.
    - Todas as atualizações de firmware ou qualquer outro software componente da solução, para a versão mais atualizada disponível ou a última compatível com as demais soluções deste lote e considerada estável.
    - Habilitação de licenças que porventura sejam adquiridas e recursos do equipamento que serão utilizados pela solução.
    - Inclusão de políticas de segurança encaminhadas pelo respectivo TRE, pré-existentes em seu ambiente, para os novos equipamentos;
5. A CONTRATADA deverá, ao final dos trabalhos, fornecer a entrega da documentação técnica completa da solução referente aos procedimentos de instalação e configuração, bem como fornecer um repasse de no mínimo 10h sobre a solução e as configurações realizadas.
6. Os serviços deverão ser realizados por técnicos credenciados pelo fabricante.
7. O fiscal técnico acompanhará os trabalhos e aprovará a documentação técnica entregue em até 10 (dez) dias corridos através de Laudo de Inspeção Técnica.
8. Após, o fiscal técnico encaminhará para o Gestor da Contratação que realizará o ateste na nota fiscal e encaminhará para pagamento no prazo de até 5 (cinco) dias corridos do recebimento do Lauto de Inspeção Técnica.

6.5.4. Para o item 5 (treinamento oficial)

a) O fornecimento desse item deverá contemplar vouchers oficiais do fabricante no Treinamento da Solução de Gerenciamento para profissionais da contratante;

b) O voucher deverá ter validade de pelo menos 12 (doze) meses, a partir da entrega e deve ser fornecido em até 20 (vinte) dias corridos após o envio da Nota de Empenho;

c) O treinamento deverá ser realizado de acordo com o calendário de treinamento do fabricante e ministrado em centro oficial de treinamento do mesmo ou remotamente, utilizando tecnologia de ensino à distância em horário comercial;

d) Deverá ser ministrado por profissional devidamente credenciado junto ao fabricante e apto a entregar o respectivo treinamento;

e) O treinamento deverá ter carga horária mínima de 40 (quarenta) horas;

f) Após a conferência do voucher, o Gestor da Contratação solicitará a emissão da nota fiscal para devido atesto e encaminhamento para pagamento.

6.6. Pagamento (Art. 18, § 3º, III, a, 7)

Após o aceite definitivo, o gestor da contratação encaminhará a nota fiscal, com o devido atesto, para o setor responsável pelo orçamento/finanças do Tribunal (no caso do TRE-AC, a Secretaria de Orçamento, Finanças e Contabilidade), para que sejam realizados os trâmites necessários para pagamento.

6.7. Transferência de Conhecimento (Art. 18, § 3º, III, a, 8)

A transferência de conhecimento será realizada por meio dos itens de implantação e treinamento existentes em cada lote.

6.8. Propriedade Intelectual (Art. 18, § 3º, III, a, 9)

As licenças de softwares, ligadas aos equipamentos, porventura fornecidas, deverão ser cedidas de forma definitiva e sem ônus futuro ao TRE-AC.

6.9. Qualificação Técnica (Art. 18, § 3º, III, a, 10)

A empresa contratada deverá apresentar a seguinte documentação complementar para fins de qualificação técnico-operacional:

a) Declaração, informando ser representante do fabricante dos equipamentos e/ou software ofertados no lote ou empresa autorizada a comercializar seus produtos;

b) Atestado de capacidade técnica, emitido por entidade de direito público ou privado, certificando que a empresa já forneceu equipamentos e serviços do tipo solicitado no lote ou similar.

A(s) empresa(s) poderá(ão) apresentar tantos atestados quantos forem necessários para comprovar o item 'b'.

A exigência referente ao item 'a' tem o intuito de evitar que a garantia do produto, geralmente atribuída ao fornecedor e não à empresa contratada, não seja válida no Brasil, caso o produto seja oriundo de importação, como é de praxe para estes tipos de equipamentos.

É importante lembrar que a maioria dos equipamentos importados, como os que compreendem o objeto do edital, têm sua garantia restrita ao território do país fabricante do produto.

Ademais, a referida declaração é de autoria da própria empresa e não do fornecedor, não restringindo a competição já que não há dependência de indicação ou escolha por parte do fornecedor, sendo passível de verificação por meio de diligência, caso seja necessária, durante o pregão eletrônico.

Quanto ao item 'b', a exigência visa preservar a integridade do Centro de Processamento de Dados (CPD) do TRE e a continuidade de seus serviços, visto que o equipamento a ser adquirido é de uso crítico e pode, em caso de manuseio inadequado, causar paralisação de serviços em produção.

6.10. Descumprimento Contratual (Art. 18, § 3º, III, a, 11)

a) A hipótese de descumprimento de prazos de entrega ou suporte previstos no item 4 deste Termo de Referência sem apresentação de justificativa, ensejará caso de inexecução parcial do objeto.

a.1) As justificativas serão analisadas pelo gestor da contratação, que opinará sobre a aceitação ou não dos motivos alegados. A aceitação será dada caso a justificativa seja baseada em problemas decorrentes de terceiros, alheios a decisões e responsabilidades da própria empresa, tais como: desastres naturais, acidentes, condições climáticas ou similares.

b) A empresa contratada ficará sujeita às sanções administrativas previstas nos arts. 86 e 87 da Lei nº 8.666/93, a serem aplicadas pela autoridade competente do TRE-AC, conforme a gravidade do caso, assegurado o direito à ampla defesa e ao contraditório, sem prejuízo do ressarcimento dos danos porventura causados à Administração e das cabíveis cominações legais.

c) No caso de inexecução total ou parcial, as seguintes sanções poderão ser aplicadas, nos termos do art. 87 da Lei nº 8.666/1993, sendo que as previstas nos incisos I, III e IV poderão ser aplicadas cumulativamente com a prevista no inciso II:

I Advertência;

II Multa prevista na forma da lei;

III Suspensão temporária de participar de licitação e/ou contratação promovida pelo TRE-AC, por prazo não superior a dois anos;

IV Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição, ou até que seja promovida a reabilitação perante a autoridade que aplicou a penalidade, que será concedida sempre que a empresa contratada ressarcir a Administração pelos prejuízos resultantes, e depois de decorrido o prazo da sanção aplicada com base no inciso anterior.

d) A inexecução total do objeto se caracterizará pela não entrega do objeto findos os prazos e condições definidos no item 6.5.

e) A inexecução parcial do objeto se caracterizará pela não entrega de parte do objeto findos os prazos e condições definidos no item 6.5, bem

como pelo disposto no item 6.10, alínea "a".

6.11. Sustentabilidade

1. Visando à efetiva aplicação de critérios, ações ambientais e socioambientais que contribuam para a promoção do desenvolvimento nacional sustentável, e em atendimento ao disposto no art. 3º da Lei n.º 8.666/93, bem como no Acórdão nº 1056/2017 – Plenário do TCU; na Resolução n.º 201/2015 do CNJ e na Resolução nº 23.474/2016 do TSE, serão exigidos os seguintes requisitos de sustentabilidade:

a) Não possuir inscrição no cadastro de empregadores flagrados explorando trabalhadores em condições análogas às de escravo, instituído pela Portaria Interministerial MTPS/MMIRDH nº 4, de 11 de maio de 2016;

b) Não ter sido condenada, empresa ou seus dirigentes, por infringir as leis de combate à discriminação de raça ou de gênero, ao trabalho infantil e ao trabalho escravo, em afronta à previsão aos artigos 1° e 170 da Constituição Federal de 1988; do artigo 149 do Código Penal Brasileiro; do Decreto n° 5.017, de 12 de março de 2004 (promulga o Protocolo de Palermo) e das Convenções da OIT nºs 29 e 105.

c) Comprovação, para os itens 1 e 2, mediante apresentação de certificação emitida por instituição pública oficial ou instituição credenciada, ou por qualquer outro meio de prova, que ateste que o produto fornecido não contém substâncias perigosas em concentração acima da recomendada na diretiva RoHS (Restriction of Certain Hazardous Substances), tais como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr(VI)), cádmio (Cd), bifenilpolibromados (PBBs), éteres difenil-polibromados (PBDEs).

d) Comprovação, para os itens 1 e 2, da regularidade do fabricante dos equipamentos junto ao Cadastro Técnico Federal de Atividades Potencialmente Poluidoras ou Utilizadoras de Recursos Ambientais;

d.1) Para comprovação, a contratada deverá informar o CNPJ da fabricante para averiguação, pelo setor demandante, da regularidade junto ao Cadastro Técnico Federal deAtividades Potencialmente Poluidoras ou Utilizadoras de Recursos Ambientais – CTF.

d.2) A exigência do Comprovante de Registro Regular no Cadastro Técnico Federal de Atividades Potencialmente Poluidoras ou Utilizadoras de Recursos Ambientais (CTF/APP) aplica-se aos fabricantes instalados no Brasil. Em se tratando de produto fabricado em outro país, compete à contratada comprovar a(s) origem(ns) do(s) produto(s).

e) Obedecer às normas técnicas, de saúde, de higiene e de segurança do trabalho, de acordo com as normas do Ministério do Trabalho e Emprego e normas ambientais vigentes.

É obrigação da contratada a manutenção dessas condições, o que poderá ser verificado constantemente durante toda a vigência do contrato, sob pena de rescisão contratual.

Em igualdade de condições, como critério de desempate, será assegurada preferência, sucessivamente, aos bens e serviços produzidos ou prestados por empresas que comprovem cumprimento de reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social e que atendam às regras de acessibilidade previstas na legislação. (Lei nº 8.666, de 1993, Art.3º, §2º, Inciso V e §5º, Inciso II; incluído pela Lei nº 13.146, de 2015, Art. 104º).

As comprovações do disposto nas alíneas “a” e “b” deverão ser feitas mediante apresentação de declaração(ões) pela empresa contratada, para fins de análise pelo setor demandante, no prazo de 24 (vinte e quatro) horas, contado a partir da confirmação do recebimento da nota de empenho.

7. ESTIMATIVA DE PREÇOS DA CONTRATAÇÃO

Estabelecido através do resultado do estudo técnico preliminar, conforme Ata de Registro de Preço 100/2022 do TRE-AC, e quantidades definidas pela equipe de contratação, segue a estimativa de preço da contratação.

ITEM	DESCRIÇÃO	QUANT	UNID	P. UNIT.	P. TOTAL
1	Firewall de Borda	1	unidade	R$ 158.152,69	R$ 158.152,69
2	Firewall de Núcleo	2	unidade	R$ 229.509,56	R$ 459019,12
3	Software de Gerenciamento e Relatório	3	unidade	R$ 4.400,00	R$ 13.320,00
4	Implantação com Hands ON	2	unidade	R$ 64.863,25	R$ 129.726,50
5	Treinamento Oficial	4	unidade	R$ 19.310,00	R$ 77.240,00
				TOTAL	R$ 837.458,31

8. ADEQUAÇÃO ORÇAMENTARIA

Encontra-se prevista a contratação, no Plano de Contratações 2023 para Cibersegurança (processo SEI nº 0002558-33.2021.6.01.8000), sob o evento 0560956.

9. DA EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO E DA APROVAÇÃO

Integrante Demandante: Silvio Forastiero Frazão

Seção de Cibersegurança - SCSEG

Integrante Técnico: Bruno Samuel Pereira Gomes

Coordenação de Infraestrutura - CIE

Integrante Administrativo: Bruna Silva Brasil

Seção de Compras Licitações e Contratos - SCLC

1A taxa de transferência (throughput) deve ser considerada com utilização de recursos necessários para reconhecimento e controle de aplicações, identificação de usuários, prevenção contra ameaças de vírus, spywares e malwares desconhecidos (Zero Day), IPS, filtro de URL, decriptografia de pacotes SSL para inspeção e recursos de VPN ativos.

2A taxa de transferência (throughput) deve ser considerada com utilização de recursos necessários para reconhecimento e controle de aplicações, identificação de usuários, prevenção contra ameaças de vírus, spywares e malwares desconhecidos (Zero Day), IPS, filtro de URL, decriptografia de pacotes SSL para inspeção e recursos de VPN ativos.

Documento assinado eletronicamente por **BRUNA SILVA BRASIL**, **Chefe de Seção**, em 30/09/2023, às 10:29, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **BRUNO SAMUEL PEREIRA GOMES SILVA**, **Coordenador(a)**, em 02/10/2023, às 09:37, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **SILVIO FORASTIERO FRAZÃO**, **Técnico Judiciário**, em 03/10/2023, às 12:20, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-ac.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0614834** e o código CRC **72E4FC19**.