TRIBUNAL REGIONAL ELEITORAL DO AMAZONAS
SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO
Coordenadoria de Infraestrutura

TERMO DE REFERÊNCIA

1. OBJETO

Registro de preços para eventual aquisição de equipamentos de infraestrutura de tecnologia da informação, com o objetivo de assegurar os requisitos de segurança da informação do Tribunal Regional Eleitoral do Amazonas, incluindo instalação, configuração, treinamento e garantia, conforme condições e especificações deste termo de referência.

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

2. JUSTIFICATIVAS

Considerando a necessidade de investimento anual em infraestrutura de TI, a presente aquisição tem como objetivo assegurar os requisitos de confidencialidade, disponibilidade e integridade das informações custodiadas do Tribunal Regional Eleitoral do Amazonas (TRE-AM), indispensáveis à continuidade do negócio e do cumprimento dos propósitos institucionais. Em suma, a presente contratação visa:

- Prover uma solução de alta disponibilidade e segurança no tráfego interno e externo da instituição;
- Prover uma solução de segurança contra-ataques na camada de rede (camada 4) e na camada de aplicação (camada 7) para a infraestrutura;
- Prover treinamento especializado da solução de segurança, garantido ao TRE-AM e seu corpo técnico conhecimento para a efetiva utilização da solução a ser adquirida.

A obtenção dos itens descritos neste termo de referência está de acordo com a estratégia de modernização empregada pela Coordenadoria de Infraestrutura, sobretudo a segurança na comunicação da rede institucional deste Tribunal.

3. CONTEÚDO DOS LOTES

Lote	Item	Descrição	Unidade	Qtd
01	**01**	Aquisição de appliance de segurança contingenciado de rede (em cluster) com suporte e manutenção do appliance de segurança contingenciado de rede (em cluster) por 5 anos.	Unidade	1
	02	Treinamento oficial da solução de segurança de rede avançada (item 1 e 2).	Unidade	4

3.1. ITEM 1 - Aquisição de appliance de segurança contingenciado de rede (em cluster) com suporte e manutenção do appliance de segurança contingenciado de rede (em cluster) por 5 anos.

3.1.1. Especificações:

3.1.1.1. O equipamento de gerência deve ser apresentado em forma de appliance, ou software e sistema operacional dedicado para a sua função.

3.1.1.2. Não serão aceitos equipamentos servidores e/ou sistemas operacionais de uso genérico, bem como gerências integradas ao Gateway de segurança.

3.1.1.3. Implementar redundância em alta disponibilidade em um conjunto de pelo menos 2 (dois) nós com fontes redundantes. Os dois nós possuirão as mesmas políticas, regras, definição de usuários, objetos de redes e configuração de sistemas.

3.1.1.4. A solução deverá ser compatível com SNMPv2 e SNMPv3;

3.1.1.5. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos equipamentos desde que obedeçam a todos os requisitos desta especificação;

3.1.1.6. A comunicação entre os appliances de segurança e o módulo de gerência deve ser através de meio criptografado;

3.1.1.7. Os appliances de segurança devem suportar operar em cluster ativo-ativo e ativo- passivo sem a necessidade de licenças adicionais;

3.1.1.8. Na data da proposta e durante a vigência do contrato, nenhum dos modelos ofertados poderá estar/ser listado no site do fabricante em listas de end-of-life, end-of-support e/ou end-of-sale;

3.1.2. Capacidade e quantidades:

3.1.2.1. A plataforma de segurança deve possuir a capacidade e as características abaixo:

3.1.2.1.1. SOLUÇÃO EM APPLIANCE DE SEGURANÇA

3.1.2.1.1.1. As especificações deste item levam em conta as medições de desempenho em ambiente real (*Enterprise Testing Conditions*). Em *datasheets* que tiverem índices de performance múltiplos será levado em consideração sempre o menor valor.

3.1.2.1.1.2. Throughput de, no mínimo, 2,2 Gbps, com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação, Antimalware e prevenção de ameaças avançadas habilitados simultaneamente;

3.1.2.1.1.3. Suporte a, no mínimo, 1.000.000 (um milhãos) de conexões simultâneas;

3.1.2.1.1.4. Suporte a, no mínimo, 50.000 (cinquenta mil) novas conexões por segundo.

3.1.2.1.1.5. Throughput de, no mínimo, 2,2 Gbps (dois), no mínimo, para conexões IPSEC-VPN;

3.1.2.1.1.6. Fonte de alimentação redundante e hot-swappable;

3.1.2.1.1.7. Armazenamento de, no mínimo 240GB SSD (Solid S

3.1.2.1.1.8. No mínimo, 8 (oito) interfaces de rede 1Gbps UTP;

3.1.2.1.1.9. No mínimo, 2 (duas) interfaces de rede 10Gbps SFP+;

3.1.2.1.1.10. Suportar, através de aquisição futura, pelo menos 2 (duas) portas 10GBase SFP+; 1 (uma) interface de rede dedicada para sincronismo; (uma) interface de rede dedicada ao gerenciamento; 1 (uma) interface do tipo console ou similar; Possuir interface dedicada para gerenciamento em caso de queda do equipamento de segurança;

3.1.2.1.1.11. Os itens 3.1.2.1.1.1 a 3.1.2.1.1.10 devem ser comprovados através de **datasheet** público na internet. É de responsabilidade da contratada indicar a página e o item da página no ***datasheet*** que comprove a conformidade com os itens técnicos solicitados. Os documentos públicos devem comprovar os throughputs aferidos com tráfego **HTTP tamanho mínimo 64Kb ou blend de protocolos definidos pelo fabricante como tráfego real (real-world traffic blend).** Para esta condição o firewall não pode ultrapassar 90% de utilização, preservando assim o investimento realizado para o projeto de 60 (sessenta) meses.

3.1.2.1.1.12. Todas as interfaces fornecidas nos appliances devem estar licenciadas e habilitadas para uso imediato, incluindo seus transceivers/transceptores. Caso sejam fornecidas interfaces além das exigidas, todas as interfaces devem ser fornecidas com todos os transceivers/transceptores necessários para a plena utilização;

3.1.2.1.1.13. Estar licenciada para ou suportar sem o uso de licença, 500 (quinhentos) clientes de VPN SSL simultâneos;

3.1.2.1.1.14. Estar licenciada para ou suportar sem o uso de licença, 500 (quinhentos) túneis de VPN IPSEC simultâneos;

3.1.2.1.1.15. A solução de *appliance* deve implementar redundância em alta disponibilidade em um conjunto de pelo menos 2 (dois) nós com fontes redundantes. Os dois nós possuirão as mesmas políticas, regras, definição de usuários, objetos de redes e configuração de sistemas.

3.1.3. Funcionalidade de firewall

3.1.3.1. A solução deve consistir de appliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW), e console de gerência e monitoração;

3.1.3.2. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões com arquitetura que garanta alta performance; A solução deve consistir de appliance de proteção de rede com funcionalidades de proteção de próxima geração;

3.1.3.3. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação técnica;

3.1.3.4. O hardware e software que executem as funcionalidades de proteção de rede deve ser do tipo appliance. Não serão aceitos equipamentos servidores e si

3.1.3.5. Os dispositivos de proteção de rede devem

funcionalidades:

3.1.3.5.1. Suporte a, no mínimo, 1024 VLAN Tags 802.1q, agregação de links 802.3ad, policy based routing ou policy based forwarding, roteamento multicast (PIM-SM), DHCP Relay, DHCP Server e Jumbo Frames;

3.1.3.5.2. A solução deve possuir mecanismo onde identifica o volume de conexões quefoi trafegada na regra, assim identificando as regras mais utilizadas;

3.1.3.5.3. Deve suportar os seguintes tipos de NAT:

3.1.3.5.3.1. Nat dinâmico (Many-to-1), Nat estático (1-to-1), Tradução de porta (PAT), NAT de Origem, NAT de Destino e suportar NAT de Origem e NAT de Destino simultaneamente;

3.1.3.5.4. Enviar logs para sistemas de monitoração externos, simultaneamente;

3.1.3.5.5. Prover mecanismo contra ataques de falsificação de endereços (IP Spoofing), através da especificação da interface de rede pela qual uma comunicação deve se originar baseado na topologia. Não sendo aceito soluções que utilizem tabela de roteamento para esta proteção;

3.1.3.5.6. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);

3.1.3.5.7. O Firewall deve ter a capacidade de operar de forma simultânea em uma unica instancia de Firewall, mediante o uso das suas interfaces fisicas nos seguintes modos: transparente, mode sniffer (monitoramento e análise o trafego de rede), camada 2 (L2) e camada 3 (L3);

3.1.3.5.8. Para IPv6, deve suportar roteamento estático e dinâmico (OSPF);

3.1.3.5.9. Suportar OSPF graceful restart;

3.1.3.5.10. Autenticação integrada via Kerberos;

3.1.3.5.11. Cada regra deve, obrigatoriamente, funcionar nas versões de endereço IPv4 e IPv6;

3.1.3.5.12. Não serão aceitas soluções nas quais as interfaces de origem e destino tenham que ser obrigatoriamente explicitadas ou obrigatoriamente listadas nas configurações deregras;

3.1.4. Funcionalidade de filtro de conteúdo web

3.1.4.1. A solução deverá contar com ferramentas licenciadas de visibilidade e controle de aplicações WEB e Filtro URL integrada no próprio appliance de segurança que permite a criação de políticas de liberação ou bloqueio baseando-se em aplicações WEB e URL;

3.1.4.2. Controle de políticas por usuários, grupos de usuários, IPs e redes;

3.1.4.3. Deve de-criptografar tráfego de entrada e saída em conexões negociadas com TLS 1.2;

3.1.4.4. Suportar a atribuição de agendamento às políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticament

3.1.4.5. Os dispositivos de proteção de rede deverão p

aplicações, independente de porta e protocolo, com as seguintes funcionalidades:

3.1.4.5.1. Deve ser possível a liberação e bloqueio de aplicações sem a necessidade de liberação de portas e protocolos;

3.1.4.5.2. Reconhecer pelo menos 2.500 (duas mil e quinhentas) aplicações diferentes, incluindo, mas não limitado a: tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, *update* de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

3.1.4.6. Para tráfego criptografado (SSL), deve de-criptografar pacotes a fim de possibilitar a leitura do payload para checagem de assinaturas de aplicações conhecidas;

3.1.4.7. A solução deve suportar a recategorização de URL's local ou adicioná-las a uma categoria personalizada;

3.1.4.8. Atualizar a base de assinaturas de aplicações automaticamente;

3.1.4.9. Limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD;

3.1.4.10. Os dispositivos de proteção de rede devem possuir a capacidade de identificaro usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários;

3.1.4.11. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos ou análise heurística;

3.1.4.12. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão;

3.1.4.13. A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:

3.1.4.13.1. Permitir especificar política por tempo, com definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

3.1.4.13.2. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes;

3.1.4.13.3. Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;

3.1.4.13.4. Deve bloquear o acesso a sites com conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, mesmo que a opção "Safe Search" esteja desabilitada no navegador do usuário;

3.1.4.13.5. Suportar base ou cache de URLs local no appliance, evitando atrasos de comunicação e validação das URLs.

3.1.4.13.6. Suportar a criação de categorias de URLs customi
Permitir a customização de página de bloqueio;

3.1.4.13.8. Como melhor pratica do uso do acesso a internet e respeitando as politicas de segurança do orgão, a ferramenta deve criar uma pagina customizada ou pop-up onde o usuário será questionado ou informado no momento do acesso a uma pagina URL ou applicação WEB de acordo com as politicas de acesso estabelecidas pela area de TI;

3.1.4.14. Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via Radius, para a identificação de endereços IP e usuários;

3.1.4.15. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no Firewall (Captive Portal);

3.1.5. Funcionalidades de prevenção de ameaças

3.1.5.1. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS (Sistema de Prevenção de Intrusão) e módulos de: Antivírus e Anti-Malware integrados no próprio equipamento de firewall;

3.1.5.2. Todas as eventuais licenças necessárias para que a solução de segurança possa executar as funcionalidades listadas neste item devem ser fornecidas.

3.1.5.3. Possuir capacidade de detecção de, no mínimo, 7.000 (sete mil) assinaturas de ataques pré-definidos;

3.1.5.4.A solução deve sincronizar ou aplicar as assinaturas de IPS, Antivírus, Anti- Malware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;

3.1.5.5.Deve suportar granularidade nas políticas de Antivírus e Anti-malware, possibilitando a criação de diferentes políticas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

3.1.5.6.A solução de IPS deve possuir análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, remontagem de pacotes de TCP e bloqueio de pacotes malformados;

3.1.5.7. Detectar e bloquear a origem de portscans;

3.1.5.8. Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações;

3.1.5.9.A solução de IPS, deve suportar a inclusão de novas assinaturas e customização no formato SNORT (ou seja, o formato SNORT pode ser convertido para o formato aceitável dentro de cada fabricante);

3.1.5.10. Possuir assinaturas para bloqueio de ataques de buffer overflow;

3.1.5.11. Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP;

3.1.5.12. Suportar bloqueio de arquivos por tipo;

3.1.5.13. Identificar e bloquear comunicação com botnets;

3.1.5.14. Deve suportar referência cruzada com CVE;

3.1.5.15. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:

3.1.5.15.1. O nome da assinatura e do ataque, aplicação, usuário, origem e o destino dacomunicação, além da ação tomada pelo dispositivo de proteção;

3.1.5.16. Deve suportar a captura de pacotes (PCAP), em assinatura de IPS e Anti-Malware, através da console de gerência centralizada;

3.1.5.17. Os eventos devem identificar o país de onde partiu a ameaça;

3.1.5.18. Deve suportar a inspeção em arquivos comprimidos (zip, gzip,etc.);

3.1.5.19. Possuir a capacidade de prevenção de ameaças não conhecidas;

3.1.5.20. Suportar a criação de políticas por Geo Localização, permitindo que o tráfego de determinado País/Países seja bloqueado;

3.1.5.21. Deve possibilitar a visualização dos países de origem e destino nos logs dosacessos;

3.1.5.22. A solução de Anti-Malware, deve ser capaz de detectar e bloquear ações decallbacks;

3.1.6. Funcionalidades de controle de qualidade de serviço

3.1.6.1. Suportar e estar licenciado para criação de políticas de QoS por:

3.1.6.1.1. Endereço de origem, endereço de destino e por porta;

3.1.6.2. O QoS deve possibilitar a definição de classes por:

3.1.6.2.1. Banda garantida, banda máxima e fila de prioridade;

3.1.6.2.2. Disponibilizar estatísticas RealTime para classes de QoS;

3.1.7. Funcionalidades de VPN

3.1.7.1. Suportar VPN Site-to-Site e Cliente-To-Site;

3.1.7.2. Suportar IPSec VPN;

3.1.7.3. Suportar SSL VPN;

3.1.7.4. A VPN IPSEc deve suportar:

3.1.7.4.1. 3DES, Autenticação MD5 e SHA-1, Diffie-Hellman Group 1, Group 2, Group 5 e Group 14, Algoritmo Internet Key Exchange (IKE), AES 128 e 256 (Advanced Encryption Standard) e Autenticação via certificado IKE PKI;

3.1.7.5. A solução deve suportar CA Interna e CA Externa de terceiros, Solução deve suportar a configuração VPN através de uma interface do tipo GUI (console do fabricante ou interface web);

3.1.8. Módulo de Gerência

3.1.8.1. Deve possuir solução de gerenciamento e administração centralizado, possibilitando o gerenciamento de diversos equipamentos de proteção de rede;

3.1.8.2. O módulo de gerência deve ser capaz de gerenciar e administrar todas as soluções descritas neste termo;

3.1.8.3. Caso a solução possua licenças relacionadas a arm

maior capacidade suportada ou ilimitada;

3.1.8.4. Caso a solução possua licenças para módulo de relatórios estendida, deve ser também entregue junto com a solução;

3.1.8.5. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo otráfego que passar pelos equipamentos da plataforma de segurança;

3.1.8.6. Centralizar a administração de regras e políticas dos equipamentos de proteção de rede, usando uma única interface de gerenciamento;

3.1.8.7.O gerenciamento da solução deve suportar acesso via SSH, cliente do própriofabricante ou WEB (HTTPS);

3.1.8.8. O gerenciamento deve permitir/possuir monitoração de logs, ferramentas deinvestigação de logs e acesso concorrente de administradores;

3.1.8.9. Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

3.1.8.10. Suportar criação de regras que fiquem ativas em horário definido e suportar criação de regras com data de expiração;

3.1.8.11. Suportar backup das configurações e rollback de configuração para a última configuração salva;

3.1.8.12. Suportar validação de regras antes da aplicação;

3.1.8.13. Suportar validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);

3.1.8.14. Deve permitir a visualização dos logs de uma regra específica em tempo real;

3.1.8.15. Deve possibilitar a integração com outras soluções de SIEM (Security information and event management – Gerenciamento de eventos e informações de segurança) de mercado;

3.1.8.16. Suportar geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;

3.1.8.17. Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e Anti-Malware), etc;

3.1.8.18. Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus, Anti-Malware), e URLs que passaram pela solução;

3.1.8.19. Deve ser possível exportar os logs em CSV;

3.1.8.20. Deve possibilitar a geração de relatórios de eventos no formato PDF;

3.1.8.21. Possibilitar rotação do log;

3.1.8.22. Suportar geração de relatórios. No mínimo os seguintes relatórios devem sergerados:

3.1.8.22.1. Resumo gráfico de aplicações utilizadas, principais aplicações por utilizaçãode largura de banda, principais aplicações por taxa de transferência de bytes, principais hosts por número de ameaças identificadas, atividades de um usuário específico e gr
aplicações acessadas, categorias de URL, URL/tempo de utili

Malware), de rede vinculadas a estetráfego;

3.1.8.23. Deve permitir a criação de relatórios personalizados;

3.1.8.24. Suportar enviar os relatórios de forma automática via PDF:

3.1.8.25. A solução de gerenciamento deverá ser entregue como appliance virtual e deve ser compatível/homologado com VMware.

3.1.8.26. Deve consolidar logs e relatórios de todos os dispositivos administrados;

3.1.8.27. Capacidade de definir administradores com diferentes perfis de acesso com,no mínimo, as permissões de Leitura/Escrita e somente Leitura;

3.1.8.28. Deverá possuir mecanismo de Drill-Down para navegação e análise dos logs em tempo real;

3.1.8.29. Nas opções de Drill-Down, deve ser possível identificar o usuário que fezdeterminado acesso;

3.1.8.30. Gerar alertas de conformidade notificando os usuários sobre o impacto desuas decisões de segurança trazendo as considerações regulatórias na gestão de segurança;

3.1.8.31. Permitir o gerenciamento eficaz das ações e recomendações, facilitando apriorização e programação de itens de ação;

3.1.8.32. Possuir recomendações de segurança acionáveis e orientações sobre como melhorar a segurança via portal de suporte ou via console de gerência.

3.1.8.33. Permitir que os relatórios possam ser salvos, enviados e impressos;

3.1.8.34. Deve incluir uma ferramenta do próprio fabricante ou de outro, ou em composição com terceiros, para correlacionar os eventos de segurança das funcionalidades adquiridas de todos os equipamentos e softwares ofertados;

3.1.8.35. Deve permitir a criação de filtros com base em qualquer característica do evento, tais como a origem e o IP destino, serviço, tipo de evento, severidade do evento, nome do ataque, o país de origem e destino, etc;

3.1.8.36. A solução deve prover, no mínimo, as seguintes funcionalidades para análise avançada dos incidentes:

3.1.8.36.1. Visualizar quantidade de tráfego utilizado de aplicações e navegação; 3.1.8.36.2. Gráficos com principais eventos de segurança de acordo com a funcionalidade selecionada;

3.1.8.37. A solução de correlação deve possuir mecanismo para controlar login de administradores em horários irregulares;

3.1.8.38. A solução deve ser capaz de detectar ataques de tentativa de login e senha gerando alertas na console ou encaminhado por e-mail ou ferramenta de terceiro;

3.1.8.39. Deve suportar a geração de relatório gerencial para apresentar aos executivos os eventos de ataque de forma completamente visual, utilizando para tanto gráficos, consumo de banda utilizado pelos ataques e quantidade de eventos gerados e protegidos;

3.1.8.40. Deve permitir a integração com servidores de autent

e Radius;

3.1.8.41. Permitir criações de políticas de acesso de usuários autenticada no Active Directory, de forma que reconheça os usuários de forma transparente;

3.1.8.42. Permitir o download de assinaturas, atualizações e firmwares para distribuição centralizada aos dispositivos de segurança integrados a mesma;

3.1.8.43. Permitir a visualização de gráficos e mapa de ameaças;

3.1.8.44. Possuir mecanismo para que logs antigos sejam removidos automaticamente;

3.1.8.45. Deve permitir a criação de dashboards customizados para visibilidades do tráfego de aplicativos, categorias de URL, ameaças, serviços, países, origem e destino;

3.1.8.46. Deve possuir a capacidade de visualizar na interface gráfica ou CLI da solução, informações do sistema como licenças, memória, disco e uso de CPU;

3.1.8.47. A solução deve ser capaz de correlacionar eventos de todas as fontes de logem tempo real;

3.1.8.48. A solução deve fornecer conteúdo de correlação pré-definido organizado porcategoria;

3.1.8.49. A solução deve possuir painéis de eventos em tempo real com possibilidade de configuração das atualizações e frequências;

3.1.8.50. Caso o fabricante não possuir os itens descritos acima, ou como solução nativa, poderá compor a solução através de outros players conhecidos;

3.2. ITEM 2 – Treinamento oficial da solução de segurança de rede avançada.

3.2.1. O treinamento deverá ser oficial do fabricante da solução do item 1 deste termo de referência. Com instrutores certificados pelo fabricante e certificados de participação do curso emitidos por centro autorizado pelo fabricante da solução.

3.2.2. O treinamento deverá ser realizado em centro autorizado.

3.2.2.1. Para realização do treinamento deverá ser no Brasil.

3.2.2.2. O treinamento não poderá ser on-line.

3.2.3. Deverá contemplar conteúdos que abranjam instalação, configuração, operação e administração da solução de segurança fornecida, bem como o uso completo (habilitação, configuração, ajustes e monitoração) de conexões VPN.

3.2.4. O conteúdo do treinamento e sua carga horária deverão ser apresentados na proposta de preço das empresas licitantes.

3.2.5. O treinamento deverá ter, no mínimo, 40 (quarenta) horas-aula, ministradas em dias úteis e em horário comercial.

3.2.6. A data do inicio do treinamento deverá ser agendada junto à Seção de Redes e Banco de Dados com antecedência mínima de 15 (quinze) dias, dentro do prazo máximo de 60 (sessenta) dias, contados da data de recebimento pela CONTRATADA da Ordem de Execução enviada pelo Fiscal

de Contrato.

3.2.7. Se o treinamento for distribuído em módulo, cada módulo deverá ser agendado com antecedência mínima de 15 (quinze) dias.

3.2.8. O prazo máximo para que a CONTRATADA finalize o treinamento será de 120 (centoe vinte) dias corridos, contados da data de recebimento, pela contratada, da Ordem de Execução emitida pelo Fiscal do Contrato.

3.2.9. Eventual alteração do conteúdo do treinamento apresentado pela CONTRATADA em sua proposta deverá ser submetida previamente para apreciação do Fiscal do Contrato.

3.2.10. A CONTRATADA será responsável:

3.2.10.1. Por providenciar o local de realização do treinamento, materiais, equipamentos e quaisquer recursos didáticos de qualidade a serem utilizados no treinamento.

3.2.10.2. Pelas despesas de deslocamento, hospedagem e alimentação do(s) instrutor(es).

3.2.10.3. Controlar a frequencia do(s) participante(s).

3.2.10.4. Emitir, sem ônus para a CONTRATANTE, o(s) certificado(s) de participação para o(s) aluno(s) que alcançar(em) o aproveitamento mínimo de (75% de presença), que deverá acompanhar a nota fiscal/fatura, para o devido pagamento, sem emendas ou rasuras, contendo a discriminação, exata do serviço prestado, valor e retenção dos impostos devidos.

3.2.11. A CONTRATANTE será responsável:

3.2.11.1. Pelas despesas de deslocamento, hospedagem e alimentação do(s) Participantes do treinamentos (Servidores).

3.2.12. Após finalização do treinamento e cumprimento, pela CONTRATADA, de todas as condições estabelecidas neste termo de referência e no Edital, o fiscal do contrato daŕa o “Atesto” nanota fiscal, certificando que os serviços foram prestados e aceitos, para fins de pagamento.

4 . MODELO DE EXECUÇÃO DO OBJETO

4.1. Instalação e configuração de equipamentos e softwares

A contratada deve ser responsável por prover os recursos necessários à instalação e configuração de equipamentos, sem ônus adicionais ao CONTRATANTE, incluindo o fornecimento de cabos elétricos, cabos lógicos, adaptadores elétricos, parafusos, porcas, conectores, kits racks, tomadas e demais materiais necessários à instalação de equipamentos nos locais de prestação dos serviços, incluindo o fornecimento de *transceivers* / *transceptores* para a utilização de interfaces de fibra-óptica.

Além dos recursos de infraestrutura supracitados, a contratada deve ser responsável pelo fornecimento de licenças de sistemas operacionais, quando *softwares* integrantes da solução proposta. Nesse contexto, in

patches de atualização, *softwares* de aplicações, *softwares* de bancos de dados, entre outros.

Ademais, os equipamentos e *softwares* necessários à prestação dos serviços devem estar cobertos por contratos de suporte técnico e garantia do fabricante durante o período de 60 (sessenta) meses.

4.2. Documentação as-built

Após a ativação dos serviços, deve ser entregue ao CONTRATANTE documentação de as-built de cada serviço, contendo as seguintes informações:

- Descrição dos serviços implantados;
- Descrição de topologia lógica e de topologia física de equipamentos após a ativação dos serviços;
- Dados dos equipamentos e *softwares*, incluindo configurações, números de série e versões;
- Parâmetros de configuração, operação, instalação, manutenção, atualização e correto funcionamento dos equipamentos e *softwares*;
- Definição de responsabilidades;
- Recursos de alta disponibilidade;
- *Scripts* de operação, incluindo desligamento e ligamento, *switch over*, acionamento do equipamento de contingência, quando necessário;
- Procedimentos para abertura e atendimento a chamados;
- Procedimentos de recuperação de equipamentos;
- Rotinas de *backup* e *restore* dos equipamentos, *softwares* e configurações implantadas;
- Rotinas periódicas configuradas;
- Documentação dos processos de trabalho associados ao item;
- Desenho dos racks onde estão instalados os equipamentos (*bayface*);
- Definição de padrões porventura existentes na solução (ex. padrão de nome de objetos)

4.3. Da garantia e do suporte técnico

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

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

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

4.3.2. 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;

4.3.3. 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;

4.3.4. 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;

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

4.3.6. 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;

4.3.7. Suporte Técnico durante o período de Garantia Técnica:

4.3.7.1. 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;

4.3.7.2. 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;

4.3.7.3. A manutenção corretiva será realizada em período int[illegible]

24 (vinte e quatro) horas por dia, após solicitação do CONTRATANTE;

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

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

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

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

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

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

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

4.3.11. A Contratada deverá garantir pleno funcionamento dos equipamentos e softwares, bem como atualizações, responsabilizando-se por qualquer componente adicional que for identificado após a contratação, seja por motivos de interoperabilidade, compatibilidade ou quaisquer outros motivos que impeçam o funcionamento efetivo da solução contratada.

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

4.3.13. A Contratada deverá garantir, sem quaisquer custos a

nos equipamentos nas versões de software e firmware, inclusive releases, pelo prazo de vigência da garantia;

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

4.3.15. As atualizações e correções (patches) do software e firmwares deverão estar disponibilizados via WEB ou fornecidas em mídia (CD ou DVD), quando desta última forma forem solicitadas.

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

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

5. CONDIÇÕES GERAIS DE FORNECIMENTO

A entrega dos materiais deverá efetuar-se na Comissão Permanente de Recebimento do TRE-AM, localizada no Edifício Sede do TRE-AM, Av. André Araújo, nº 200, Aleixo, CEP 69060-000, Manaus – AM, de segunda a sexta-feira, no horário das 08 às 14h.

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

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

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;

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-AM.

6. OBRIGAÇÕES

6.1. Caberá à CONTRATANTE:

6.1.1. Prestar informações e esclarecimentos pertinentes e necessários que venham a ser solicitados pelo representante da CONTRATADA;

6.1.2. Efetuar os pagamentos à CONTRATADA nos prazos previstos na legislação em vigor, após o cumprimento das formalidades legais;

6.1.3. Emitir o aceite do objeto contratado após verificação das especificações, rejeitando o que não estiverde acordo, por meio de notificação à CONTRATADA;

6.1.4. Relacionar-se com a contratada exclusivamente por meio de pessoa por ela indicada.

6.2. Caberá à CONTRATADA:

6.2.1. Responsabilizar-se por todos os encargos tributários, previdenciários, fiscais e comerciais decorrentes do fornecimento, bem como, pelos danos causados diretamente à Administração ou a terceiros, decorrentes de sua culpa ou dolo na entrega dos materiais contratados, não excluindo ou reduzindo essa responsabilidade o acompanhamento pela Administração do TRE-AM;

6.2.2. Substituir e/ou refazer, às suas expensas, todo e qualquer equipamento que estiver em desacordo com as especificações (e/ou aquele em que for constatado dano em decorrência de transporte ou acondicionamento), após a notificação formal do CONTRATANTE;

6.2.3. Manter as condições de habilitação e qualificação exigidas para sua contratação;

6.2.4. Arcar com todas as despesas diretas e indiretas, decorrentes do cumprimento das obrigações assumidas sem qualquer ônus adicional para o CONTRATANTE;

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

7. PRAZO DE ENTREGA

O prazo de entrega dos materiais será de no máximo 60 (sessenta) dias corridos, a contar da data da retirada da correspondente Nota de Empenho.

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/ justificadamente, e apresentada até o último dia do referido pr

8. ESTRATÉGIA DA CONTRATAÇÃO

8.1. Critério de julgamento e proposta de preços

8.1.1. Será considerada vencedora a proposta com o MENOR VALOR GLOBAL, para fins de registro de preços.

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

8.1.1.2. 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. Nesse sentido, justifica-se o agrupamento em lote, uma vez que entendemos ser a opção mais vantajosa à administração e satisfatória do ponto de vista da eficiência técnica, por manter a qualidade do projeto, haja vista que o gerenciamento e execução técnica permanece todo o tempo a cargo de um mesmo fornecedor.

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

8.1.1.4. Isto posto, o agrupamento em lote visa garantir a compatibilidade técnica e operacional entre os componentes da solução, visto que haverá integração entre software e hardware existente no TRE-AM.

8.1.2. A proposta de preços deve ser apresentada conforme modelo do ANEXO I deste termo de referência.

8.2. Critérios de qualificação técnica para habilitação

8.2.1. A LICITANTE deverá apresentar pelo menos 01 (um) atestado de capacidade técnica, fornecido por pessoa jurídica de direito público ou privado, que comprove o fornecimento e implantação de solução de appliance de segurança contingenciado de rede (em cluster) com suporte e manutenção, a fim de comprovar a aptidão para desempenho de atividade pertinente e compatível com o objeto da licitação.

8.2.2. Os atestados deverão conter as seguintes informações m
os assina, quantitativo associado ao fornecimento, valor e/ou C

dos serviços;

8.2.3. 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.

8.2.4. Conforme art. 43, §3º da Lei nº 8.666/93, os conteúdos dos atestados/declarações poderão ser objeto de averiguação pelo TRE-AM, mediante diligências.

8.2.5. Ainda, em termos de diligência, o TRE-AM 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.

9. PAGAMENTO

O pagamento será realizado em até 05 (cinco) 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 Comissão de Recebimento do TRE-AM, por meio de depósito em conta corrente, mediante Ordem Bancária.

A Nota Fiscal deverá ser apresentada devidamente preenchida e discriminada, em nome do Tribunal Regional Eleitoral do Amazonas, CNPJ nº 05.959.999/0001-14 e remetida via protocolo ao setor solicitante.

10. SANÇÕES

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

a) Deixar de entregar a documentação exigida no Edital;

b) Não assinar a Ata de Registro de Preços ou o contrato e/ou não receber a Ordem de Fornecimento e/ou de Serviço;

c) Apresentar documento falso ou fizer declaração falsa;

d) Causar atraso na execução do objeto deste Pregão;

e) Não 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 nº 8.666/93, pelo atraso injustificado e inexecução total ou parcial do objeto deste Pregão, a Administração do Tribunal Regional Eleitoral do Amazonas poderá, garantida a defesa prévia, aplicar à licitante vencedora as seguintes sanções:

a) Advertência, nas hipóteses de faltas leves, assim entendidas aquelas que não acarretem prejuízos para o TRE/AM;

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

c) Multa compensatória de até 10% (dez por cento) sobre o valor global do respectivo material, na hipótese de recusa em receber a Ordem de Fornecimento e/ou de Serviço;

d) Multa compensatória de até 10% (dez por cento) sobre o valor global do respectivo material, na hipótese de inexecução parcial ou total da obrigação.

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

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

Rubens Antônio Pinto Soares
Técnico Judiciário

Marcelo de Jesus Ferreira
Analista Judiciário

De acordo:

Mayara Santos Santos
Coordenadora de Infraestrutura

Assinado eletronicamente conforme Lei 11.419/2006
Em: 09/06/2022 09:31:05
Por: MAYARA SANTOS SANTOS

TRE

ANEXO I

MODELO DE PROPOSTA COMERCIAL

Proposta que faz a empresa _____ inscrita no CNPJ _____, localizada no endereço_____, na cidade de_____, telefone_____, fax_____, e-mail _____, para o FORNECIMENTO EQUIPAMENTOS DE INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO, INCLUINDO INSTALAÇÃO, CONFIGURAÇÃO, TREINAMENTO E GARANTIA,_____, de acordo com todas as especificações e condições estabelecidas no pregão eletrônico e anexos.

Lote	Item	Unidade	Descrição	Quantidade Registrada	Valor Unitario (R$)	Valor Total(R$) Do lote
1	1	UN	Aquisição de appliance de segurança contingenciado de rede (em cluster) com suporte e manutenção do appliance de segurança contingenciado de rede (em cluster) por 5 anos.	1		
	2	UN	Treinamento oficial da solução de segurança de rede avançada (item 1 e 2).	4		
VALOR GLOBAL DA PROPOSTA						

A empresa_____declara que concorda com todas as especificações do edital e seus anexos.

PRAZO DE VALIDADE DA PROPOSTA: 60 DIAS

Obs.: Nos preços acima propostos estão inclusas todas as despesas e custos diretos e indiretos, como impostos, taxas, fretes e garantia dos equipamentos.

CIDADE:_____ESTADO: _____

DATA:_____/_____/_____

NOME DA EMPRESA E CNPJ

ANEXO II

MINUTA DA ATA DE REGISTRO DE PREÇOS

ATA DE REGISTRO DE PREÇOS N.º_____/2022

Aos_____dias do mês de_____do ano de dois mil e vinte e dois a UNIÃO, por intermédio do TRIBUNAL REGIONAL ELEITORAL DO AMAZONAS, inscrito no CNPJ/MF sob o n.º 05.959.999/0001-18, com sede provisória na Av. André Araújo, nº 200, Aleixo, CEP 69060-000, Manaus – AM, doravante designado CONTRATANTE, neste ato representado por seu Diretora-Geral, _____, no uso da atribuição que lhe foi atribuída regimentalmente, resolve REGISTRAR OS PREÇOS dos materiais permanentes licitados mediante o Pregão SRP nº_____/2022, sob o regime de aquisição pelo sistema de registro de preços, a fim de atender às necessidades deste Tribunal, nos termos das Leis nº 8.666/93, 10.520/02 e do Decreto 7.892/2013, e suas alterações, em conformidade com as cláusulas e condições que se seguem.

CLÁUSULA PRIMEIRA: ITENS E FORNECEDORES REGISTRADOS

1.1- A partir desta data, ficam registrados neste Tribunal os preços dos fornecedores abaixo indicados, objetivando o compromisso de fornecimento dos bens constantes do quadro abaixo, nas condições estabelecidas no ato convocatório.

Lote	Item	Descrição	Qtde. Estimada	Valor Unitário
Empresa vencedora: CNPJ: Endereço: Telefone/fax: Email: Representante: CPF:				

1.2 - A existência de preços registrados não obriga este Tribunal a contratar, sendo facultada a realização de licitação específica para a aquisição pretendida, assegurado ao beneficiário do registro a preferência de fornecimento em igualdade de condições, conforme disposição contida no Edital de Licitação do Pregão nº_/2022.

CLÁUSULA SEGUNDA: EXPECTATIVA DE FORNECIMENTO

2.1 - Os Materiais com preços registrados serão adquiridos de acordo com a necessidade e conveniência deste Tribunal, mediante a emissão da respectiva Nota de Empenho de despesa, decorrente desta Ata de Registro de Preços e observadas as disposições contidas no Edital do Pregão SRP nº_/2022.

2.2 - O fornecedor fica obrigado a atender todos os pedidos efetuados durante a validade desta Ata de Registro de Preços.

2.3 - A empresa fornecedora deverá retirar a Nota de Empenho no prazo máximo de 3 (três) dias a contar da comunicação deste Tribunal, sob pena de decair o seu direito à contratação, sem prejuízo das sanções legais cabíveis.

2.3.1 - Tratando-se de empresa sediada fora do município de Manaus-AM, a Nota de Empenho será enviada via fax ou e-mail, devendo a empresa fornecedora retornar o empenho pelos mesmos meios enviados, com o devido recebimento.

2.4 - O prazo máximo de entrega dos materiais é de 60 (sessenta) dias, a contar da retirada da Nota de Empenho.

CLÁUSULA TERCEIRA: CONTROLE DOS PREÇOS REGISTRADOS:

3.1 - O TRE/AM adotará a prática de todos os atos necessários ao controle e administração da presente Ata.

3.2 - Os preços registrados e a indicação do respectivo fornecedor detentor da Ata serão divulgados em meio eletrônico, no portal de internet deste Tribunal: www.tre-am.jus.br

CLÁUSULA QUARTA: VIGÊNCIA

4.1 - O prazo de vigência da presente Ata é de 12 (doze) meses a contar da data da sua publicação.

CLÁUSULA QUINTA: FORO E NORMAS VINCULANTES

5.1 - Fica definido o Foro da Justiça Federal na cidade de Manaus-AM para dirimir os conflitos que possam ocorrer no presente compromisso.

5.2 - As normas que vinculam o compromisso são o Termo de Referência elaborado pela COINF/STI/TRE-AM, o Edital de Licitação Modalidade Pregão nº_/2022, as Leis nº 8.666/93, 10.520/2002 e o Decreto nº 7.892/2013.

Manaus-AM,___de_____de 2022.

_____

Diretora-Geral do TRE-AM

_____

Representante do Fornecedor