TRIBUNAL REGIONAL ELEITORAL DO AMAZONAS

SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO
COORDENADORIA DE INFRAESTRUTURA

TERMO DE REFERÊNCIA

1 – OBJETO

A presente licitação tem como objetivo a formação de Ata de Registro de Preços para Solução unificada de gestão de vulnerabilidades em ativos de tecnologia da informação e aplicações web, compreendendo aquisição de serviços de software e suporte técnico, de acordo com as quantidades, especificações e condições descritas neste Termo de Referência.

2 – JUSTIFICATIVA

O registro de preços objetiva a dotar o corpo técnico do TRE-AM de ferramentas que auxiliam na detecção e priorização de tratamento de vulnerabilidades nos ativos de TIC (Roteadores, switches, estações de trabalho, hosts do ambiente de virtualização, bancos de dados, máquinas virtuais, sistemas operacionais, servidores de aplicações, aplicações Web etc).

3 – DA PADRONIZAÇÃO DOS SOFTWARES E LICENÇAS

3.1. Conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (*I - Atender ao principio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas*), todos os softwares e licenças das soluções ofertadas em cada lote deverão ser fornecidos por um único fabricante, o qual será responsável também pelo suporte e garantia da plataforma como um todo.

4 – COMPOSIÇÃO

LOTE ÚNICO - **Solução com armazenamento e gerenciamento local (On Premise)**			
ITEM	**QTD**	**CATMAT / CATSER**	**DESCRIÇÃO**
01	1	24333	Licenciamento de plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando no mínimo 500 endereços IP, por 60 meses de uso e suporte pelo fabricante.

02	1	24333	Licenciamento para solução de análise dinâmica em aplicações Web, pacote para no mínimo 10 domínios (FQDN), por 60 meses de uso e suporte pelo fabricante.
03	1	26972	Instalação e configuração da solução.
04	1	26972	Repasse tecnológico, com período mínimo de 20 horas.
05	50	26972	4 Horas de Serviço Especializado.

Especificações técnicas:

4.1 REQUISITOS GERAIS DA SOLUÇÃO

Características técnicas mínimas:

4.1.1. A solução deve estar licenciadas e inclusas todas as funcionalidades para realizar varreduras (scans) de vulnerabilidades, avaliação de configuração e conformidade (baseline e compliance), indícios e padrões de códigos maliciosos conhecidos (malware);
4.1.2. A solução deve possuir recurso de varredura ativa, onde o scanner comunica-se com os alvos (ativos) através da rede;
4.1.3. A solução de gestão de vulnerabilidades deve suportar varreduras de dispositivos de IoT;
4.1.4. Deve ser capaz de identificar no mínimo 50.000 CVEs (Common Vulnerabilities and Exposures);
4.1.5. A solução deve ter a capacidade de adicionar etiquetas (tags) aos ativos de maneira automática, manual e possibilitar o uso de regras com parâmetros específicos para aplicação das mesmas;
4.1.6. Deve atribuir a todas as vulnerabilidades uma severidade baseada no CVSSv3 score;
4.1.7. A solução deve calcular a criticidade com base nos dados agregados e consolidados do ativo, dados de segurança, sistema e conformidade, bem como hierarquias e prioridades;
4.1.8. A solução deve fornecer criptografia de ponta a ponta dos dados de vulnerabilidades;
4.1.9. A solução deve possuir a capacidade de armazenar informações dos ativos descobertos no ambiente;
4.1.10. Deve possuir um sistema de busca de informações de um determinado ativo com no mínimos as seguintes características:
4.1.10.1. Por sistema operacional;
4.1.10.2. Por um determinado software instalado;
4.1.10.3. Por Ativos impactados por uma determinada vulnerabilidade.
4.1.11. A solução deve possuir suporte para a adição de detecções personalizadas usando o OVAL (Open Vulnerability Assessment Language);
4.1.12. Deve permitir aceitar o risco de uma determinada vulnerabilidade encontrada no ambiente;
4.1.13. Possibilitar alterar a criticidade de determinada vulnerabilidade de forma manual;

4.1.14. A solução deve possuir um sistema de pontuação e priorização das vulnerabilidades;
4.1.15. A solução deve ser capaz de aplicar algoritmos de aprendizagem de máquina (machine learning) para analisar as características relacionadas a vulnerabilidades;
4.1.16. O sistema de pontuação e priorização de vulnerabilidades deve avaliar no mínimo as seguintes características:
4.1.16.1. CVSSv3 Impact Score;
4.1.16.2. Idade da Vulnerabilidade;
4.1.16.3. Se existe ameaça ou exploit que explore a vulnerabilidade;
4.1.16.4. Número de produtos afetados pela vulnerabilidade;
4.1.17. Deve ser capaz de fazer a correlação em tempo real de ameaças ativas contra vulnerabilidades encontradas, incluindo feeds de inteligência de ameaças ao vivo;

4.1.18. Deve possuir uma API para automação de processos e integração com aplicações terceiras permitindo, no mínimo, a extração de dados para carga no SIEM.

4.1.19. Deve possuir uma API para automação de processos e integração com aplicações ITSM do órgão para as vulnerabilidades encontradas, permitindo o agrupamento no chamado por ações corretivas;

4.1.20. A solução deve permitir a instalação de agentes em estações de trabalho e servidores, para varredura diretamente no sistema operacional;
4.1.21. A solução deve ser capaz de produzir relatórios nos seguintes formatos: PDF, CSV e HTML;
4.1.22. A solução deve possuir recurso de monitoria passiva do tráfego de rede para identificação de anomalias, novos dispositivos e desvios de padrões observados;
4.1.23. A solução deve ser licenciada para o uso ilimitado de sensores passivos de rede para realizar o monitoramento em tempo real;

4.1.24. A solução deve possuir sensores, no mínimo, com as seguintes funcionalidades:

a. Execução de verificação completa do sistema (rede), adequada para qualquer host;
b. verificação sem recomendações da rede, para que se possa personalizar totalmente as configurações da verificação;
c. Autenticação de hosts e enumeração de atualizações ausentes;
d. Execução de varredura simples para descobrir hosts ativos e portas abertas;
e. Utilização de um scanner para verificar aplicativos da web;
f. Avaliação de dispositivos móveis
g. Auditoria de configuração de serviços em nuvem de terceiros;
h. Auditoria de configuração dos gerenciadores de dispositivos móveis;
i. Auditoria de configuração dos dispositivos de rede;
j. Auditoria de configurações do sistema em relação a uma linha de base conhecida;
k. Detecção de desvio de segurança Intel AMT;
l. Verificação de malware nos sistemas Windows e Unix;

4.1.25. Deve ser possível determinar em tempo real quais portas de serviços (UDP/TCP) estão abertas em determinado ativo;
4.1.26. A solução deve ser capaz de realizar em tempo real a descoberta de novos ativos para no

mínimo:
a) Bancos de dados;
b) Hypervisors (no mímino VMWare ESX/ESXi);
c) Dispositivos móveis;
d) Dispositivos de rede;
e) Endpoints;
f) Aplicações;
4.1.27. A solução deve ser capaz de em tempo real detectar logins e downloads de arquivos em um compartilhamento de rede;

4.1.28. Permitir identificar vulnerabilidades associadas a servidores SQL no tráfego de rede;
4.1.29. A solução deve possuir interface para integração com as principais soluções de SIEM de mercado, tais como IBM QRadar, Microfocus ArcSight e Splunk.
4.1.30. A solução deve possibilitar a realização de cópias de segurança, funcionamento em alta disponibilidade e criptografia de todos os dados armazenados, além de incluir todo o software e licenciamento necessários para o funcionamento completo de acordo com as funcionalidades previstas neste Termo de Referência.
4.1.31. A atualização das ameaças deve ocorrer diariamente e sem interrupção dos serviços.
4.1.32. Configuração de segurança e acesso à gerência da solução:
a) Todos os dados armazenados nos servidores da solução devem ser criptografados e possuir logs de acesso;

b) Os dados em trânsito devem usar ao menos o algoritmo TLS 1.2 de chave 2048 bits;

c) Os dados em trânsito devem ser criptografados ao menos com o algoritmo AES-128 bits;

d) Os algoritmos de hash devem usar ao menos o algoritmo SHA-256;

e) Será aceito como comprovação critérios de criptografia publicação em site do fabricante ou declaração do próprio fabricante;

e) Os dados armazenados devem ser criptografados ao menos com o algoritmo AES-256 bits;

f) Somente servidores da Contratante ou pessoa por ela autorizada poderão ter acesso aos dados da solução;
g) A solução deve permitir a criação de, no mínimo, 20 contas para gerência e acesso aos relatórios, sem custo adicional;

h) A empresa contratada não deverá ter acesso a rede interna da contratante e todo trafego de dados deverá ser de saída e iniciado pelos scanners (on-premise).

4.1.33. Todas as licenças de uso de software devem ser registradas, na data da entrega, em nome da Contratante no site do fabricante.
4.1.34. Dos Relatórios:
4.1.34.1. Deve ser capaz de executar relatórios periódicos de acordo com a frequência estabelecida pelo administrador, bem como a geração de relatórios sob demanda;
4.1.34.2. A solução deve possibilitar a criação de relatórios baseados na seleção de ativos, permitindo inclusive a seleção de todos os ativos existentes;
4.1.34.3. Deve suportar a criação de relatórios criptografados (protegidos por senha configurável) ;

4.1.34.4. A solução deve suportar o envio automático de relatórios para destinatários específicos;
4.1.34.5. Deve ser possível definir a frequência na geração dos relatórios para no mínimo: Diário, Mensal, Semanal e Anual;
4.1.34.6. Permitir especificar níveis de permissão nos relatórios para usuários e grupos específicos;
4.1.34.7. A solução deve fornecer relatórios do tipo “scorecard” para as partes interessadas da empresa;
4.1.34.8. A solução deve fornecer relatórios de correções aplicadas, classificados pelos seguintes critérios: grupo de ativos, usuários e vulnerabilidades;
4.1.35. A solução deve permitir mecanismo de varredura baseado em inferência com técnicas de varredura não intrusivas;
4.1.36. A solução deve possuir ou permitir a criação de relatórios com as seguintes informações:
4.1.36.1. Hosts verificados sem credenciais;
4.1.36.2. Top 100 Vulnerabilidades mais criticas;
4.1.36.3. Top 10 Hosts infectados por Malwares;
4.1.36.4. Hosts exploráveis por Malwares;
4.1.36.5. Total de vulnerabilidades que podem ser exploradas pelo Metasploit;
4.1.36.6. Vulnerabilidades críticas e exploráveis;
4.1.36.7. Máquinas com vulnerabilidades que podem ser exploradas;
4.1.37. A solução deve possuir dashboards customizáveis onde o administrador pode criar, editar ou remover painéis de acordo com a necessidade;
4.1.38. A solução deve ser capaz de inventariar todos os ativos da rede local e publicados na Internet, sem limites de endereços IPs.
4.1.39. O fornecedor assinará, no ato da entrega das licenças e do serviço, Termo de Confidencialidade, em que se comprometerá a não acessar, não divulgar e proteger todos os dados de infraestrutura e de vulnerabilidades do contratante a que tiver acesso, que abrangerá todos os seus colaboradores e terceiros, sob as penas da lei.

4.2 CARACTERÍSTICAS PLATAFORMA DE SOFTWARE PARA GESTÃO DE VULNERABILIDADES

Características técnicas mínimas:

4.2.1. A plataforma de software deve ser capaz de realizar varreduras (scans) de vulnerabilidades, de acordo com a quantidade de endereços IP licenciados;
4.2.2. A plataforma de software deve ser licenciada para um número ilimitado de scanners (prevendo redundância);
4.2.3. Deve permitir a configuração de vários painéis e widgets;
4.2.4. Deve ser capaz de medir e reportar ameaças;
4.2.5. Deve ser capaz de visualizar ameaças críticas ao ambiente monitorado;
4.2.6. A plataforma de software deve realizar varreduras em uma variedade de sistemas operacionais, suportando pelo menos hosts baseados em Windows, Linux e Mac OS, bem como appliances virtuais;
4.2.7. A plataforma de software deve suportar vários mecanismos de varredura distribuídos em

diferentes localidades e regiões e gerenciar todos por uma console central;
4.2.8. A plataforma de software deve fornecer agentes instaláveis em sistemas operacionais, pelo menos Windows, Linux e Mac OS, para o monitoramento contínuo de configurações e vulnerabilidades;
4.2.9. A plataforma de software deve permitir o monitoramento através de agentes instalados, até o limite de licenças adquiridas, para varredura diretamente no sistema operacional.

4.2.10. A plataforma de software deve permitir o monitoramento sem a necessidade de agentes instalados, até o limite de licenças adquiridas, para varredura diretamente no sistema operacional.
4.2.11. A plataforma de software deve incluir a capacidade de programar períodos de tempo e data onde varreduras não podem ser executadas, como por exemplo em determinados dias do mês ou determinados horários do dia;
4.2.12. No caso onde uma atividade de varredura seja interrompida por invadir o período não permitido, o mesmo deve ser capaz de ser reiniciado de onde parou;
4.2.13. A plataforma de software deve ser configurável para permitir a otimização das parametrizações de varredura;
4.2.14. A plataforma de software deve permitir a entrada e o armazenamento seguro de credenciais do usuário, incluindo contas locais, de domínio (LDAP e Active Directory) e root para sistemas Linux;
4.2.15. A plataforma de software deve fornecer a capacidade de escalar privilégios nos destinos, do acesso de usuário padrão até acesso de sistema ou administrativo;
4.2.16. A plataforma de software deve ser capaz de realizar pesquisas de dados confidenciais.

4.3 CARACTERÍSTICAS DE ANÁLISE DINÂMICA EM APLICAÇÕES WEB

Características técnicas mínimas:

4.3.1. A solução de análise deve realizar varreduras de vulnerabilidades em aplicações Web, cobrindo no mínimo, mas não limitando-se a base de ameaças apontadas pelo OWASP Top 10, CWE e WASC;
4.3.2. A solução de análise deve ser capaz de analisar, testar e reportar falhas de segurança em aplicações Web;
4.3.3. A solução de análise deverá ser capaz de executar varreduras em sistemas Web através de seus endereços IP ou FQDN (DNS);
4.3.4. A solução de análise deve ser capaz de identificar vulnerabilidades de divulgação de dados, como vazamento de informações de identificação pessoal;
4.3.5. Para varreduras do tipo extensas e detalhadas, deve varrer e auditar no mínimo os seguintes elementos:
a) Cookies, Headers, Formulários e Links;
b) Nomes e valores de parâmetros da aplicação;
c) Elementos JSON e XML;
d) Elementos DOM;
4.3.6. Deverá também permitir a execução da função crawler, que consiste na navegação para descoberta das URLs existentes na aplicação;
4.3.7. A solução de análise deve suportar a integração com o softwares de automação de testes para

permitir sequências de autenticação complexas;
4.3.8. A solução de análise deve ser capaz de realizar testes/varreduras em aplicações separadas, simultaneamente limitadas ao número de licenças;
4.3.9. A solução de análise deve oferecer suporte à capacidade de testar novamente a vulnerabilidade específica que foi detectada anteriormente no aplicativo Web;
4.3.10. Deve ser capaz de utilizar scripts customizados de crawling com parâmetros definidos pelo usuário;
4.3.11. Deve ser capaz de excluir determinadas URLs da varredura através de expressões regulares;
4.3.12. Deve ser capaz de excluir determinados tipos de arquivos através de suas extensões;
4.3.13. Deve ser capaz de instituir no mínimo os seguintes limites:
a) Número máximo de URLs para crawling e navegação;
b) Número máximo de diretórios para varreduras;
) Tamanho máximo de respostas;
e) Tempo máximo para a varredura;
4.3.14. Deve ser capaz de agendar a varredura e determinar sua frequência entre uma única vez, diária, semanal, mensal e anual;
4.3.15. Deve suportar o envio de notificações por email;
4.3.16. Deverá ser compatível com avaliação de web services REST e SOAP;
4.3.17. A solução de análise deve suportar os seguintes esquemas de autenticação:
a) Autenticação Básica (Digest);
b) NTLM;
c) Autenticação de Cookies;
4.3.18. A solução de análise deve ser capaz de exibir os resultados das varreduras de forma temporal para acompanhamento de correções e introdução de novas vulnerabilidades;
4.3.19. Os resultados devem ser apresentados agregados por vulnerabilidades ou por aplicações;
4.3.20. Para cada vulnerabilidade encontrada, deve ser exibido detalhes e evidências;
4.3.21. Cada vulnerabilidade encontrada deve conter também soluções propostas para mitigação ou remediação;
4.3.22 A solução de análise deve fornecer relatórios de resumo geral de todas as aplicações web e resumo de uma aplicação específica, que serão exportados para os formatos XML, HTML ou PDF.
4.3.23. A solução deve ser capaz de realizar varreduras nos seguintes componentes/aplicações:
a. WordPress;
b. IIS 6.x e IIS 10.x;
c. ASP 6;
d. NET 2;
e. Apache HTTPD 2.2.x e 2.4.x;
f. Tomcat 6.x, 7.x, 8.x e superiores;
g. Jetty 8 e superiores;
h. Nginx;
i. PHP 5.3.x, 5.4.x, 5.6.x, 7.0.x e 7.1.x e superiores;
j. Java 1.5, 1.6, 1.7 e 1.8 e superiores;
k. Jboss 4.x e 7.x e superiores;
l. WildFly 8 e 10 e superiores;
m. Plone 2.5.x e 4.3.x e superiores;

n. Zope;
o. Python 2.4.4 e superiores;
p. J2EE;
q. Ansible;
r. Joomla;
s. Moodle;
t. Docker Conteiner;
u. Elk;
v. GIT;
w. Grafana; e
x. Redmine.

4.4 INSTALAÇÃO E CONFIGURAÇÃO

Características técnicas mínimas:

4.4.1. Efetuar as configurações iniciais, em conjunto com a Contratante, para uso da solução proposta, incluindo criação de scans, relatórios, filtros, permissões de usuários e demais funcionalidades da solução;
4.4.2. Apoio na instalação de scanners e agentes on-premises;

4.4.3. A instalação e configuração da solução poderá ser feita por meio de acesso remoto;

4.4.4. A CONTRATADA deverá aceitar as especificações de softwares e protocolos de segurança estabelecidos pela CONTRATANTE para a realização do acesso remoto;

4.4.5. Não serão aceitos softwares “beta” ou em desenvolvimento;

4.4.6. Somente será aceita a instalação por técnico certificado na fabricante da solução, da CONTRATADA ou do fabricante;
4.4.7. A CONTRATADA deverá elaborar documentação, contendo no mínimo os seguintes itens:
4.4.7.1 Cronograma;
4.4.7.2 Levantamento de informações sobre o ambiente atual;
4.4.7.3 Definição dos parâmetros de configuração básicos e avançados a serem implementados;
4.4.7.4 Mapa de rede contendo a topologia a ser implementada ou atualizada;
4.4.7.5 Gerenciamento de mudanças, contemplando análise de riscos de implementação da solução;
4.4.7.6 Procedimentos de implementação e de rollback no caso de problemas não previstos previamente.

4.4.8 A CONTRATADA poderá subcontratar uma empresa autorizada pelo fabricante para atender as atividades relacionadas ao Instalação e Configuração (itens 11 do lote 01 e item 24 do lote 02).

4.5 REPASSE TECNOLÓGICO

Características técnicas mínimas:

4.5.1. A contratada deverá ministrar treinamento, na língua portuguesa, para até 10 (dez) servidores indicados pelo órgão, com carga horária mínima de 20 horas.

4.5.2. O conteúdo do treinamento a ser ministrado deverá contemplar os seguintes itens:

a. Procedimentos de instalação física e lógica;
b. Todos os procedimentos necessários à configuração técnica;
c. Todos os procedimentos necessários à completa operação do produto; e
d. Todos os procedimentos de manutenção do produto que devem ser realizados pelos técnicos do órgão.

4.5.3. O treinamento poderá ser realizado virtualmente por profissional certificado pelo fabricante do produto ofertado;

4.5.4. O treinamento deverá ser ministrado em horário definido pelo tribunal, em dias úteis;
4.5.5. O treinamento será dado como concluído após a avaliação dos participantes, com o preenchimento da Planilha de Avaliação de Treinamento, devendo ser obtida média superior a 70%, caso contrário a CONTRATANTE poderá solicitar a realização de novo treinamento, com a reformulação que achar necessária.

4.5.6 A CONTRATADA poderá subcontratar uma empresa autorizada pelo fabricante para atender as atividades relacionadas ao Repasse Tecnológico.

4.6 Bloco de 04 Horas de Serviço Especializado

Características técnicas mínimas:

4.6.1 A operação assistida e consultoria especializada será solicitada pela contratante sob demanda e prestada por meio de acesso remoto, de acordo com as necessidades elencadas, nos dias úteis (de segunda a sexta-feira), no horário de 08hs as 18hs, e deverão executar as seguintes atividades:

a. Acompanhar, quando solicitado por um usuário, todas as operações realizadas no sistema durante determinado período de tempo;
b. Esclarecer dúvidas de usuários em relação à operação do sistema;
c. Prestar serviços de suporte técnico para a solução de problemas que impeçam o perfeito funcionamento do sistema;
d. Reportar à Coordenação de informática do órgão quaisquer outros problemas verificados durante o atendimento, relativos ou não à solução fornecida;
e. Fornecer informações aos usuários sobre a situação e o andamento de serviços de manutenção solicitados;
f. Diagnosticar a performance do software em seus aspectos operacionais;
g. Identificar problemas inerentes ao software e ao ambiente onde este se encontra instalado;
h. Discutir implementações de melhorias, visando possíveis adequações;
i. Na prestação dos serviços de operação assistida, a Contratada deverá utilizar profissionais com qualificação e treinamento adequados para o desenvolvimento das tarefas relacionadas anteriormente;
j. apoio no desenvolvimento de dashboad´s e solução de problemas internos, relativos às licenças

adquiridas.
k. Integração da solução com ferramentas de ITSM.
l. Documentação e transferência de conhecimento das atividades técnicas realizadas.

4.6.2 A CONTRATADA deverá aceitar as especificações de softwares e protocolos de segurança estabelecidos pela CONTRATANTE para a realização do acesso remoto.

4.6.4 A CONTRATADA poderá subcontratar uma empresa autorizada pelo fabricante para atender as atividades relacionadas ao Bloco de 04 Horas de Serviço Especializado .

4.7 OUTROS REQUISITOS ESPECÍFICOS DA SOLUÇÃO COM GERENCIAMENTO E ARMAZENAMENTO NA REDE LOCAL

Características técnicas mínimas:

4.7.1. Os Solução deverá possuir gerenciamento e armazenamento dos dados na rede local do tribunal, com scanners próprios localizados e instalados na infraestrutura do cliente (on-premise).

4.7.2. A aquisição da plataforma de software de gestão de vulnerabilidades é pré-requisito para a contratação do módulo de análise dinâmica de aplicações web.

4.7.3. A solução proposta deve ser de mesmo fabricante, sem adaptações ou alterações não efetuadas pelo fabricante, disponível para gerenciamento em console central unificado.
4.7.4. A solução deve ser licenciada para uso perpétuo. As funcionalidades da solução devem permanecer ativas após o período de garantia mesmo que desatualizadas e com todas as atualizações e assinaturas que forem disponibilizadas até data final do período que foram aplicadas ou instaladas na solução;

5 – DAS CONDIÇÕES DE INSTALAÇÃO E GARANTIA

5.1 – Do local onde os softwares e licenças poderão ser entregues e instalados:

5.1.1. Sede do Tribunal
Av. ANDRÉ ARAÚJO, 200 - ALEIXO – MANAUS/AM
CEP: 69060-000 - AMAZONAS – Brasil
Telefone: (92) 3632-4400

5.2 – Condições de participação e realização dos serviços

5.2.1. A solução será constituída de softwares, licenças e serviços relacionados nos itens do lote, sendo todos de um mesmo fabricante, garantindo a entrega e execução dos serviços por uma única empresa e a total compatibilidade entre eles;
5.2.2. A escolha do agrupamento dos itens em lote visa que a empresa fornecedora que prestará os serviços de fornecimento será a mesma que prestará os serviços de instalação, configuração, repasse tecnológico e consultoria especializada durante a vigência do contrato de garantia dos softwares e

licenças, garantindo a total compatibilidade entre os softwares solicitados e a capacidade técnica de manter a solução em operação.

5.3 – Garantia e suporte técnico

5.3.1. Os softwares e licenças fornecidos deverão estar cobertos por garantia que ofereça atualizações necessárias para a correção de vícios, pelo período especificado no termo de referência, a contar da data do aceite provisório do software, conforme Art. 73, I, "a", da Lei 8.666/1993;

5.3.1.1 O suporte pelo fabricante será obrigatório;

5.3.1.2 O suporte pela CONTRATADA será opcional e ela poderá subcontratar uma empresa autorizada pelo fabricante para prestar o suporte técnico de primeiro nível;

5.3.2. Devem estar explícitos na proposta os part numbers de garantia oficial do fabricante no Brasil;

5.3.3 O tempo da garantia e suporte técnico estarão explicitadas nas especificações específicas dos respectivos itens.

5.3.4. A empresa deve indicar, na assinatura do contrato, os procedimentos para abertura de suporte técnico, cabendo a este órgão a abertura do chamado com intermediação da empresa fornecedora dos produtos ou diretamente com o fabricante;

5.3.5. A empresa deve possuir, no momento da assinatura do contrato, pelo menos 1 (um) profissional com certificação técnica emitida pelo fabricante, capaz de prestar o Serviço Especializado SOLICITADO nos itens;

5.3.6. Os chamados telefônicos deverão estar disponibilizados de segunda à sexta-feira, das 8 às 18 horas, adotando-se para tanto o horário de Brasília;

5.3.6.1 O tempo para a resposta dos chamados dependerá da severidade do problema conforme abaixo:

5.3.6.2 Não poderá ser superior a 2 horas, após abertura do chamado, para problemas com severidade crítica (Funcionalidade do produto completamente degradada, impacto crítico nas operações);

5.3.6.3 Não poderá ser superior a 12 horas, após abertura do chamado, para problemas com severidade alta (Funcionalidade do produto severamente degradada, impacto severo nas operações);

5.3.6.4 Não poderá ser superior a 2 (dois) dias úteis, após abertura do chamado, para problemas com severidade média (Erros, problemas gerais, produto danificado, no entanto, as operações permanecem funcionais);

5.3.7. A empresa contratada ou o fabricante deverão disponibilizar, cumulativamente, abertura de suporte técnico por meio de atendimento telefônico, website e e-mail;

5.3.8. Os serviços de garantia aos produtos deverão ser prestados por empresa credenciada pelo fabricante ou pelo próprio fabricante dos produtos fornecidos.

5.3.9. A contratada ou o fabricante deverão disponibilizar um portal web com disponibilidade de 24 horas por dia, 7 dias por semana e 365 dias por ano, com sistema de help-desk para abertura de

chamados de suporte técnico;
5.3.10. 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;
5.3.11. Os chamados abertos por e-mail deverão ter sua abertura automática no portal web;
5.3.12. Todo o chamado aberto deverá ter sua resolução técnica registrada no sistema web de help-desk;
5.3.13. A contratante poderá solicitar o escalonamento de incidentes ao fabricante quando se tratarem de correções especiais, defeitos nos programas ou defeito em hardware;
5.3.14. A contratada poderá prestar o suporte técnico dos produtos, sendo facultado a ela o escalonamento das questões para o respectivo fabricante, ficando, entretanto, a contratada responsável pelo gerenciamento do chamado e prestação de informações junto à contratante;

5.3.15. A garantia iniciará sua contagem a partir da data de emissão da NF dos softwares, serviços ou licenças;
5.3.16. Havendo discrepâncias entre o que está especificado no item específico e o que consta nestas condições gerais, prevalecerá o que está no item específico.

5.4 - Atualizações

5.4.1. A contratada deverá disponibilizar, na vigência do contrato, todas as atualizações dos softwares dos componentes da solução, concebidas em data posterior ao seu fornecimento, pelo período especificado no item constante do termo de referência (60 meses), sem qualquer ônus adicional para o contratante;
5.4.2. As atualizações incluídas devem ser do tipo “minor release” e “major release”, permitindo manter todos componentes atualizados em sua última versão de software/firmware.

5.5 - Condições de entrega e recebimento

5.5.1. O fornecimento das licenças de software deverá ocorrer em até 05 (cinco) dias úteis após a assinatura do contrato.

5.5.2. A instalação, configuração, customização, criação de relatórios, filtros, criação de dashboards para gestão e operação deverão ocorrer em até 05 (cinco) dias úteis após o fornecimento das licenças de software.

5.5.3. O repasse tecnológico de 20 horas será agendado conforme disponibilidade de agenda das partes, podendo ser efetuado em outro exercício financeiro, mas em prazo não superior a 90 dias da data de assinatura do contrato e a contratada terá um prazo de 5 dias úteis para iniciar a prestação do serviço após o recebimento da solicitação.

5.5.4. O Bloco de 04 horas de Serviço Especializado será solicitado sob demanda pelo contratante e a contratada terá um prazo de 24 horas para iniciar a prestação do serviço após o recebimento da solicitação.

5.5.5. A entrega deve ser agendada com antecedência mínima de 24 horas, sob o risco de não ser autorizada;

5.5.6. Os serviços devem ser agendados com antecedência mínima de 5 dias sob o risco de não ser autorizado;

5.5.7. Para itens de software, devem ser fornecidos com ou sem a mídia de instalação. No caso de não fornecimento de mídia, deve ser indicado local para download do arquivo de instalação;

5.5.8. Para itens de software, devem ser apresentados chave única tipo serial ou qualquer outra forma de validação da ferramenta, comprovando perante o fabricante que trata-se de uma ferramenta devidamente licenciada;
5.5.9. O Termo de Recebimento Provisório será emitido por servidor ou comissão do TRE-AM, devidamente constituída para este fim, em **até 5 dias úteis após a entrega dos itens**;
5.5.9. O Termo de Recebimento Definitivo será emitido por servidor ou comissão do TRE-AM devidamente constituída para este fim **em até 10 dias úteis após a entrega.**

5.6 - Condições de aceite

5.6.1. O aceite do bem somente será dado após comprovação da entrega e o efetivo cumprimento de todas as exigências da presente especificação técnica;

5.6.2. Para comprovação de pleno atendimento aos requisitos deste edital, serão consultados folhetos, prospectos, manuais e toda documentação pública disponível diretamente do site do fabricante. Em caso de dúvida ou divergência na comprovação da especificação técnica, este órgão poderá solicitar amostra do produto ofertado, sem ônus ao processo, para comprovação técnica de funcionalidades. Esta amostra deverá ocorrer em até 5 (cinco) dias úteis após a solicitação deste órgão.

5.7 - Condições de pagamento

5.7.1. O pagamento será feito por etapas, ao final da conclusão de cada uma delas, que estão descritas nas especificações dos itens que o compõem.

6 - HABILITAÇÃO E QUALIFICAÇÃO DO FORNECEDOR

6.1. A PROPONENTE deverá:
6.1.1. Comprovar pertencer ao ramo de atividade pertinente ao objeto da contratação, através de cartão CNPJ, estatuto ou contrato social em vigor devidamente registrado na Junta Comercial;
6.1.2. Comprovar aptidão do desempenho de atividade pertinente e compatível em tecnologia com a solução global especificada neste Termo de Referência. A comprovação deverá acontecer através de:
6.1.2.1. Apresentação de declaração do fabricante da solução ofertada no lote garantindo que a empresa revendedora é capaz de fornecer, instalar, configurar e prestar suporte da solução ofertada, não implicando em perda de garantia no Brasil e;
6.1.2.2 Atestados ou certidões de capacidade técnica, em nome da licitante, expedidos por pessoas jurídicas de direito público ou privado, registrado nas entidades profissionais competentes, que

comprove o regular fornecimento, instalação e configuração de solução de gestão/gerenciamento de vulnerabilidade, que compreenda no mínimo fornecimento e instalação dos produtos em quantidade igual ou superior a 50% dos produtos constantes do lote ofertado neste certame, sendo da mesma marca da solução que pretende fornecer à este órgão no âmbito da presente contratação.

6.1.3. Possuir no mínimo 1 (um) profissional com certificação técnica oficial do fabricante da solução que pretende fornecer a este órgão no âmbito da presente contratação;
6.1.3.1. O técnico deverá estar devidamente contratado pela empresa fornecedora da solução.
6.1.4. O licitante deverá comprovar, através do Public Sector Addendum (PSA), válido, que está habilitado a realizar vendas ou prestar serviços do fabricante junto a clientes do setor público.
6.2. Todas as comprovações exigidas neste item deverão ser enviadas durante a fase de habilitação.

7 - DAS PENALIDADES

7.1 - O CONTRATANTE poderá aplicar à CONTRATADA as penalidades previstas no artigo 49 do Decreto nº 10.024/2019. A Administração poderá, ainda, a seu critério, utilizar-se subsidiariamente das sanções previstas na Lei nº 8.666/93, no que couber.
7.2. A recusa injustificada do adjudicatário em assinar o contrato, se for o caso, no prazo de 05 (cinco) dias, contados da notificação do CONTRATANTE, caracteriza o descumprimento total da obrigação assumida, sujeitando-o à penalidade de multa no percentual de até 30% (trinta por cento) sobre o valor global da obrigação não cumprida.
7.3 - Fica estabelecido como falta grave, caracterizado como falha em sua execução, a não manutenção de todas as condições de habilitação e qualificação exigidas na licitação, que poderá dar ensejo à rescisão do contrato, sem prejuízo da aplicação da multa compensatória estabelecida no item 13.3 e do impedimento para licitar e contratar com a União, nos termos do art. 49 do Decreto nº 10.024/2019.
7.4 - Com fundamento no art. 49 do Decreto nº 10.024/2019, ficará impedida de licitar e contratar com a União e será descredenciada no SICAF, pelo prazo de até 5 (cinco) anos, sem prejuízo das demais cominações legais e de multa compensatória de até 30% (trinta por cento), no caso de inexecução total, sobre o valor total da contratação, ou de até 15% (quinze por cento), no caso de inexecução parcial, sobre o valor do saldo da contratação, respectivamente, a Contratada que:
7.4.1 - não assinar o contrato ou a ata de registro de preços;
7.4.2 - não entregar a documentação exigida no edital;
7.4.3 - apresentar documentação falsa;
7.4.4 - causar o atraso na execução do objeto;
7.4.5 - não mantiver a proposta;
7.4.6 - falhar na execução do contrato;
7.4.7 - fraudar a execução do contrato;
7.4.8 - comportar-se de modo inidôneo;
7.4.9 - declarar informações falsas; e
7.4.10 - cometer fraude fiscal.
7.5 - Para os fins do item 7.4.8, reputar-se-ão inidôneos atos como os descritos nos arts. 90, 92, 93, 94, 95 e 97 da Lei nº 8.666/93.

7.6 - A Contratada ficará sujeita, no caso de inexecução parcial ou total da obrigação, com fundamento no art. 86 da Lei nº 8.666/93, à seguinte penalidade:
7.7.1 - multa moratória de:
7.7.1.1 - 0,05% (zero vírgula zero cinco por cento) ao dia sobre o valor do contrato em caso de atraso na execução do serviço, limitada a incidência de 10 (dez) dias;
7.7.1.2 - Sendo o atraso superior a 10 (dez) dias, configurar-se-á inexecução total da obrigação, a ensejar a aplicação da multa compensatória, prevista no item 13.3, sem prejuízo da aplicação da multa moratória limitada a 0,5% (zero vírgula cinco por cento), oriunda do atraso referido no subitem anterior, bem como da rescisão unilateral da avença.

8. CLASSIFICAÇÃO DOS BENS COMUNS

8.1 - Os bens a serem adquiridos enquadram-se na classificação de bens comuns, nos termos da Lei n° 10.520, de 2002, do Decreto n° 3.555, de 2000, e no Decreto 10.024/2019.

9. VIGÊNCIA DA ATA DE REGISTRO DE PREÇOS E DO VALIDADE DO CONTRATO:

9.1. A(s) ata(s) de registro de preços decorrente(s) desta contratação terão validade de 12 (doze) meses.
9.2. O(s) contrato(s) decorrentes das ARP´s terá(ão) vigência de 60 meses.

10. OBRIGAÇÕES DA CONTRATADA

Além das demais obrigações descritas ao longo deste Termo de Referência, a CONTRATADA obriga-se a:

10.1. Fornecer todas as licenças de software necessárias para utilização completa da solução, pelos períodos adquiridos.
10.2. Registrar, junto aos fabricantes e em nome da contratante, todas as assinaturas de licenças de software ofertadas.

10.3. Cumprir fielmente as obrigações assumidas, conforme as especificações constante neste Termo de Referência, utilizando-se de todos os recursos materiais e humanos necessários para entregar os produtos/prestar os serviços, nos prazos indicados.
10.4. 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, por ocasião da entrega dos objetos licitados no local indicado, incluindo os possíveis danos causados por transportadoras, sem qualquer ônus ao contratante.
10.5. Prestar todos os esclarecimentos que forem solicitados pelo TRE-AM, credenciando junto ao órgão, um representante para prestar os devidos esclarecimentos e atender as reclamações que porventura surgirem durante a execução do objeto.
10.6. Assinar, através de seu responsável legal, Termo de Sigilo e Responsabilidade, garantindo o sigilo e a confidencialidade dos dados a que vier a ter contato durante a instalação e durante a

utilização da solução de software.

10.7. A contratada obrigar-se-á em manter-se em compatibilidade com a habilitação e com as obrigações assumidas na licitação até o adimplemento total da contratação.

10.8. Executar os serviços nos prazos estabelecidos neste instrumento, nos locais indicados pela Administração, em estrita observância das especificações do Edital e da proposta;
10.9. Atender prontamente aos chamados da Administração, relacionados ao objeto da licitação;
10.10. Comunicar à Administração, no prazo máximo de 24 (vinte e quatro) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação;
10.11. Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;
10.12. Responsabilizar-se pelas despesas dos tributos, encargos trabalhistas, previdenciários, fiscais, comerciais, taxas, fretes, seguros, deslocamento de pessoal, prestação de garantia e quaisquer outras que incidam ou venham a incidir na execução do contrato.
10.13 Apresentar junto com a Fatura/Nota Fiscal dos serviços prestados, as comprovações de regularidade junto à Seguridade Social (CND), ao Fundo de Garantia por Tempo de Serviço (CRF) e às Fazendas Federal, Estadual e Municipal de seu domicílio ou sede, bem como a Certidão Negativa de Débitos Trabalhistas de que trata a Lei nº 12.440/2011; caso esses documentos não estejam disponíveis no SICAF.
10.14 Não transferir a terceiros, por qualquer forma, nem mesmo parcialmente, as obrigações assumidas, nem subcontratar qualquer das prestações a que está obrigada, exceto nos casos e condições autorizadas pelo CONTRATANTE, já previstos neste Termo de Referência.

11. OBRIGAÇÕES DA CONTRATANTE

A Contratante obriga-se a:
11.1. Receber provisoriamente o material, disponibilizando local, data e horário.
11.2.Verificar minuciosamente, no prazo fixado, a conformidade dos bens recebidos provisoriamente com as especificações constantes do Edital e da proposta, para fins de aceitação e recebimento definitivos.
11.3. Acompanhar e fiscalizar o cumprimento das obrigações da Contratada, através do gestor e dos fiscais especialmente designados.
11.4. Efetuar o pagamento na forma e no prazo previsto neste instrumento e no contrato.

12. ADJUDICAÇÃO DO OBJETO

12.1 - A adjudicação será feita por lote, tendo em vista tratam-se de soluções não divisíveis e por comporem soluções tecnológicas, bem como para fins de garantir total compatibilidade entre os itens agrupados.

13 - LOGÍSTICA REVERSA

13.1. É de responsabilidade da CONTRATADA a disposição final responsável e ambientalmente adequada das embalagens e dos materiais após o uso, em observância à Logística Reversa disposta no art. 33 da Lei Nº 12.305/2010 - que institui a Política Nacional de Resíduos Sólidos;
13.2. O Tribunal reserva-se o direito de assumir a responsabilidade a que se refere o item anterior, podendo dar outra destinação às embalagens e materiais após o uso, caso julgue mais conveniente para a Administração;
13.3. Os materiais utilizados na embalagem do produto ofertado deverão ter sua reciclabilidade efetiva no Brasil.

RODRIGO PINTO DE CARVALHO

COORDENADORIA DE INFRAESTRUTURA