Estudos Técnicos Preliminares

Apresentamos a seguir aspectos a considerar tecnicamente acerca da necessidade de aquisição descrita no Documento de Oficialização de Demanda (vide Doc nº 76762/2020 – PAD 7917/2020).

Caracterização da Demanda

1. Descrição da Solução de TIC a ser contratada

Registro de preço para contratação de ferramenta de Gestão de Vulnerabilidades.

2. Equipe de planejamento da contratação

Integrante	Nome	Ramal	E-mail	Setor
Demandante	*RODRIGO PINTO DE CARVALHO*	4469	rodrigo.carvalho@tre-am.jus.br	COINF
Administrativo	EUZEBIO RODRIGUES CARDOSO JUNIOR	4448	euzebio.cardoso@tre-am.jus.br	SEAU
Técnico	RUBENS ANTÔNIO PINTO SOARES	5560	rubens.soares@tre-am.jus.br	SEPD

3. Necessidade da contratação

O monitoramento das vulnerabilidades de segurança num ambiente computacional é absolutamente necessário para se manter a confidencialidade, a disponibilidade e a integridade das informações. Neste contexto, buscamos implementar uma solução de software capaz de testar os ativos de TI e as aplicações web periodicamente em busca de quaisquer vulnerabilidades, sejam elas relativas a atualização de sistemas operacionais e servidores de aplicação, configurações de serviços ou outras falhas técnicas. Além disso, é preciso que a solução forneça relatórios para que seja possível o acompanhamento deste trabalho de identificação e mitigação de riscos.

4. Alinhamento estratégico

Ação prevista no desdobramento do atual Planejamento estratégico de TI do TRE-AM, Processos internos – Conformidade e Integração – Primar pela satisfação dos usuários internos de TIC. Nivelamentos tecnológico.

Temas relacionados no PETI: Prover e aprimorar infraestrutura para os serviços de TIC

Aperfeiçoar a gestão de TIC Atendimento às normas vigentes do âmbito da Justiça eleitoral e poder judiciário

Seção I - Análise da Viabilidade da Contratação

5. Requisitos da contratação

O presente estudo objetiva a contratação de ferramenta de gestão de vulnerabilidades para atender as necessidades do Tribunal Regional Eleitoral do Amazonas.

5.1 Necessidades do negócio

Necessidade: Gerenciamento de Vulnerabilidades em Sistemas Operacionais*;*

Funcionalidade: Testar os hosts (físicos e virtuais), comparando a bases de dados de vulnerabilidades mantidas por organizações especializadas em segurança da informação e por grandes fabricantes de software*;*

Ator(es) Envolvido(s): STI/COINF.

Necessidade: Gerenciamento de Vulnerabilidades em Sistemas e páginas Web;

Funcionalidade: Testar as aplicações e páginas web, internas e externas, comparando a bases de dados de vulnerabilidades mantidas por organizações especializadas em segurança da informação e por grandes fabricantes de software;

Ator(es) Envolvido(s): STI/CDES

Necessidade: Emissões de Relatórios;

Funcionalidade: Emitir relatórios de acompanhamento dos testes e das vulnerabilidades encontradas, apontando quando forem solucionadas;

Ator(es) Envolvido(s): STI/COINF

5.2 Requisitos Tecnológicos e Não Funcionais

5.2.1. Requisitos Tecnológicos

5.2.1.1. 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) para no mínimo 250 IPs;

5.2.1.2. A solução deve possuir recurso de varredura ativa, onde o scanner comunica-se com os alvos (ativos) através da rede;

5.2.1.3. A solução de gestão de vulnerabilidades deve suportar varreduras de dispositivos de IoT;

5.2.1.4. Deve ser capaz de identificar no mínimo 50.000 CVEs (Common Vulnerabilities and Exposures);

5.2.1.5. 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;

5.2.1.6. Deve atribuir a todas as vulnerabilidades uma severidade baseada no CVSSv3 score;

5.2.1.7. 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;

5.2.1.8. A solução deve fornecer criptografia de ponta a ponta dos dados de vulnerabilidades;

5.2.1.9. A solução deve possuir a capacidade de armazenar informações dos ativos descobertos no ambiente;

5.2.1.10. Deve possuir um sistema de busca de informações de um determinado ativo com no mínimos as seguintes características:

5.2.1.10.1. Por sistema operacional;

5.2.1.10.2. Por um determinado software instalado;

5.2.1.10.3. Por Ativos impactados por uma determinada vulnerabilidade.

5.2.1.11. A solução deve possuir suporte para a adição de detecções personalizadas usando o OVAL (Open Vulnerability Assessment Language);

5.2.1.12. Deve permitir aceitar o risco de uma determinada vulnerabilidade encontrada no ambiente;

5.2.1.13. Possibilitar alterar a criticidade de determinada vulnerabilidade de forma manual;

5.2.1.14. A solução deve possuir um sistema de pontuação e priorização das vulnerabilidades;

5.2.1.15. A solução deve ser capaz de aplicar algoritmos de aprendizagem de máquina (machine learning) para analisar as características relacionadas a vulnerabilidades;

5.2.1.16. O sistema de pontuação e priorização de vulnerabilidades deve avaliar no mínimo as seguintes características:

5.2.1.16.1. CVSSv3 Impact Score;

5.2.1.16.2. Idade da Vulnerabilidade;

5.2.1.16.3. Se existe ameaça ou exploit que explore a vulnerabilidade;

5.2.1.16.4. Número de produtos afetados pela vulnerabilidade;
5.2.1.17. Deve ser capaz de fazer a correlação em tempo real de ameaças ativas contra vulnerabilidades encontradas, incluindo feeds de inteligência de ameaças ao vivo;

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

5.2.1.19. 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;

5.2.1.20. A solução deve permitir a instalação de agentes em estações de trabalho e Servidores, para varredura diretamente no sistema operacional;
5.2.1.21. Se for baseada em nuvem, a solução deve possuir conectores para, no mínimo, as seguintes plataformas:
a) Amazon Web Service (AWS);
b) Microsoft Azure;
c) Google Clound Platform.

5.2.1.22. A solução deve ser capaz de produzir relatórios nos seguintes formatos: PDF, CSV ou HTML;
5.2.1.23. A solução deve possuir recurso de monitoria passiva do tráfego de rede para identificação de anomalias, novos dispositivos e desvios de padrões observados;
5.2.1.24. A solução deve ser licenciada para o uso ilimitado de sensores passivos de rede para realizar o monitoramento em tempo real;

5.2.1.25. 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;

5.2.1.26. Deve ser possível determinar em tempo real quais portas de serviços (UDP/TCP) estão abertas em determinado ativo;
5.2.1.27. A solução deve ser capaz de realizar em tempo real a descoberta de novos ativos para no minímo:
a) Bancos de dados;
b) Hypervisors (no mímino VMWare ESX/ESXi);
c) Dispositivos móveis;
d) Dispositivos de rede;
e) Endpoints;
f) Aplicações;

5.2.1.28. A solução deve ser capaz de em tempo real detectar logins e downloads de arquivos em um compartilhamento de rede;

5.2.1.29. Permitir identificar vulnerabilidades associadas a servidores SQL no tráfego de rede;
5.2.1.30. A solução deve possuir interface para integração com as principais soluções de SIEM de mercado, tais como IBM QRadar, Microfocus ArcSight e Splunk.

5.2.1.31. 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.
5.2.1.32. A atualização das ameaças deve ocorrer diariamente e sem interrupção dos serviços.
5.2.1.33. 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 transito devem usar ao menos o algoritimo TLS 1.2 de chave 2048 bits;

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

d) Os algoritimos de hash devem usar ao menos o algoritimo 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 algoritimo 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-premises).

5.2.1.34. Todas as licenças de uso de software devem ser registradas, na data da entrega, em nome da Contratante no site do fabricante.
5.2.1.35. Dos Relatórios:
5.2.1.35.1. Deve ser capaz de executar relatórios periódicos de acordo com a frequência estabelecida pelo administrador, bem como a geração de relatórios sob demanda;
5.2.1.35.2. A solução deve possibilitar a criação de relatórios baseados na seleção de ativos, permitindo inclusive a seleção de todos os ativos existentes;
5.2.1.35.3. Deve suportar a criação de relatórios criptografados (protegidos por senha configurável) ;
5.2.1.35.4. A solução deve suportar o envio automático de relatórios para destinatários específicos;
5.2.1.35.5. Deve ser possível definir a frequência na geração dos relatórios para no mínimo: Diário, Mensal, Semanal e Anual;
5.2.1.35.6. Permitir especificar níveis de permissão nos relatórios para usuários e grupos específicos;
5.2.1.35.7. A solução deve fornecer relatórios do tipo “scorecard” para as partes interessadas da empresa;
5.2.1.35.8. A solução deve fornecer relatórios de correções aplicadas, classificados pelos seguintes critérios: grupo de ativos, usuários e vulnerabilidades;
5.2.1.36. A solução deve permitir mecanismo de varredura baseado em inferência com técnicas de varredura não intrusivas;
5.2.1.37. A solução deve possuir ou permitir a criação de relatórios com as seguintes informações:
5.2.1.37.1. Hosts verificados sem credenciais;
5.2.1.37.2. Top 100 Vulnerabilidades mais criticas;
5.2.1.37.3. Top 10 Hosts infectados por Malwares;
5.2.1.37.4. Hosts exploráveis por Malwares;
5.2.1.37.5. Total de vulnerabilidades que podem ser exploradas pelo Metasploit;
5.2.1.37.6. Vulnerabilidades críticas e exploráveis;
5.2.1.37.7. Máquinas com vulnerabilidades que podem ser exploradas;
5.2.1.38. A solução deve possuir dashboards customizáveis onde o administrador pode criar, editar ou remover painéis de acordo com a necessidade;
5.2.1.39. A solução deve ser capaz de inventariar todos os ativos da rede local e publicados na Internet, sem limites de endereços IPs.
5.2.1.40. A plataforma de software deve ser capaz de realizar varreduras (scans) de vulnerabilidades para no mínimo 250 IPs;
5.2.1.41. A plataforma de software deve ser licenciada para um número ilimitado de scanners (prevendo redundância);
5.2.1.42. Deve permitir a configuração de vários painéis e widgets;
5.2.1.43. Deve ser capaz de medir e reportar ameaças;
5.2.1.44. Deve ser capaz de visualizar ameaças críticas ao ambiente monitorado;
5.2.1.45. 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;
5.2.1.46. A plataforma de software deve suportar vários mecanismos de varredura distribuídos em diferentes localidades e regiões e gerenciar todos por uma console

central;
5.2.1.47. 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;
5.2.1.48. A plataforma de software deve permitir o monitoramento através de agentes instalados, até o limite de licenças adquiridas, para varredura diretamente no sistema operacional.

5.2.1.49. 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.
5.2.1.50. 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;
5.2.1.51. 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;
5.2.1.52. A plataforma de software deve ser configurável para permitir a otimização das parametrizações de varredura;
5.2.1.53. 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;
5.2.1.54. A plataforma de software deve fornecer a capacidade de escalar privilégios nos destinos, do acesso de usuário padrão até acesso de sistema ou administrativo;
5.2.1.55. A plataforma de software deve ser capaz de realizar pesquisas de dados confidenciais;

5.2.1.56. A solução deve possuir módulo para realizar análise dinâmica em aplicações Web:

5.2.1.56.1 A solução deve possuir módulo para realizar varreduras de vulnerabilidades para no mínimo 5 aplicações Web, cobrindo no mínimo, mas não limitando-se a base de ameaças apontadas pelo OWASP Top 10, CWE e WASC:

5.2.1.56.2. A solução de análise deve ser capaz de analisar, testar e reportar falhas de segurança em aplicações Web;
5.2.1.56.3. A solução de análise deverá ser capaz de executar varreduras em sistemas Web através de seus endereços IP ou FQDN (DNS);
5.2.1.56.4. A solução de análise deve ser capaz de identificar vulnerabilidades de divulgação de dados, como vazamento de informações de identificação pessoal;
5.2.1.56.5. 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;
5.2.1.56.6. Deverá também permitir a execução da função crawler, que consiste na navegação para descoberta das URLs existentes na aplicação;
5.2.1.56.7. A solução de análise deve suportar a integração com o softwares de

automação de testes para permitir sequências de autenticação complexas;
5.2.1.56.8. A solução de análise deve ser capaz de realizar testes/varreduras em aplicações separadas, simultaneamente limitadas ao número de licenças;
5.2.1.56.9. A solução de análise deve oferecer suporte à capacidade de testar novamente a vulnerabilidade específica que foi detectada anteriormente no aplicativo Web;
5.2.1.56.10. Deve ser capaz de utilizar scripts customizados de crawling com parâmetros definidos pelo usuário;
5.2.1.56.11. Deve ser capaz de excluir determinadas URLs da varredura através de expressões regulares;
5.2.1.56.12. Deve ser capaz de excluir determinados tipos de arquivos através de suas extensões;
5.2.1.56.13. 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;
c) Número máximo de elementos DOM;
d) Tamanho máximo de respostas;
e) Tempo máximo para a varredura;
f) Número máximo de conexões HTTP(S) ao servidor hospedando a aplicação Web;
g) Número máximo de requisições HTTP(S) por segundo;
5.2.1.56.14. Deve ser capaz de agendar a varredura e determinar sua frequência entre uma única vez, diária, semanal, mensal e anual;
5.2.1.56.15. Deve suportar o envio de notificações por email;
5.2.1.56.16. Deverá ser compatível com avaliação de web services REST e SOAP;
5.2.1.56.17. A solução de análise deve suportar os seguintes esquemas de autenticação:
a) Autenticação Básica (Digest);
b) NTLM;
c) Autenticação de Cookies;
5.2.1.56.18. Deve ser capaz de importar scripts de autenticação previamente configurados pelo usuário;
5.2.1.56.19. 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;
5.2.1.56.20. Os resultados devem ser apresentados agregados por vulnerabilidades ou por aplicações;
5.2.1.56.21. Para cada vulnerabilidade encontrada, deve ser exibido detalhes e evidências;
5.2.1.56.22. Cada vulnerabilidade encontrada deve conter também soluções propostas para mitigação ou remediação;
5.2.1.56.23. Serviço de Detecção de Malware:
a) A solução de análise deve utilizar a plataforma de gerenciamento de vulnerabilidades existente;
b) A solução de análise deve permitir visualizar o acompanhamento das atividades de verificação, páginas infectadas e tendências de infecção por malware;
c) 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.

5.2.1.56.24. 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 5.2.1.41.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.

5.2.2. Requisitos de Capacitação

A contratação deve possuir um item de repasse tecnológico com no mínimo 20 horas para capacitar os servidores da STIC a operacionalizar a ferramenta.

5.2.3. Requisitos Legais

5.2.3.1 - Margem de Preferência

Não há.

5.2.4. Requisitos de Manutenção

Não há requisitos de manutenção dos itens adquiridos, exceto quando houver mudança de versão do sistema operacional.

5.2.5. Requisitos Temporais

5.2.5.1. Prazos

5.2.5.1.1. O licitante terá 5 (cinco) dias contados da assinatura do contrato para fornecer os softwares ou as subscrições contratadas;

5.2.5.1.2. O atraso não justificado deverá ser punido de acordo com as sanções aplicadas ao contrato.

5.2.5.2. Suporte e garantia

A garantia de atualização do software deve ser de, no mínimo, 60 (sessenta) meses, contados do dia seguinte ao vencimento do suporte em vigência dos itens constantes no portal do fabricante.

5.2.6. Requisitos de Segurança

5.2.6.1. A empresa contratada deverá respeitar as diretrizes constantes da Política de Segurança da Informação do da Justiça Eleitoral (Resolução TSE Nº 23.501/2016), obrigando-se a manter sigilo a respeito de quaisquer informações, dados, processos, fórmulas, códigos, cadastros, fluxogramas, diagramas lógicos, dispositivos, modelos ou outros materiais de propriedade do Tribunal Regional Eleitoral do Amazonas aos quais tiver acesso em decorrência do objeto da presente contratação, ficando terminantemente proibida de fazer uso ou revelação destes sob qualquer justificativa;

5.2.6.2. O Tribunal Regional Eleitoral do Amazonas terá propriedade sobre todos os documentos e procedimentos operacionais produzidos no escopo da presente contratação;

5.2.6.3. Os documentos eventualmente produzidos deverão ser repassados ao Tribunal tanto em formato não editável (PDF) como também em formato editável (.DOCX).

5.2.6.4. 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.

5.2.7. Requisitos Sociais, Ambientais e culturais

5.2.7.1. Logística Reversa

5.2.7.1.1. É de responsabilidade da CONTRATADA a disposição final responsável e ambientalmente adequada das embalagens e materiais que porventura venham a ser utilizados em observância à Logística Reversa disposta no art. 33 da Lei Nº 12.305/2010, que institui a Política Nacional de Resíduos Sólidos;

5.2.7.1.2. 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;

5.2.7.1.3. Qualquer material que venha a ser utilizado na embalagem dos produtos ofertados e/ou utilizados na execução dos serviços deverão ter sua reciclabilidade efetiva no Brasil.

6. Levantamento das Alternativas Disponíveis no Mercado

As soluções presentes no presente estudo resumem-se as seguintes opções.

6.1. Soluções

6.1.1. Utilização de softwares livres

Nome da Solução: Softwares livres OpenVas e Nmap

Fornecedor: Comunidades Open Source e páginas específicas dos projetos.

Descrição: Utilizar ferramentas livres ou gratuitas, como os softwares OpenVas e Nmap.

6.1.2. Solução paga com gerenciamento e armazenamento na nuvem (On Cloud)

Nome da Solução: Ferramenta de Gestão de Vulnerabilidades On Cloud

Fornecedores: Qualys (Cotação 0834401), Tenable (Cotação 0834081) e Rapid7 (Cotação 0834093)

Descrição: Aquisição de software de gerenciamento de vulnerabilidades e análise dinâmica de aplicações web baseado em nuvem, com modelo de subscrição por 60 meses.

6.1.3. Solução paga com gerenciamento e armazenamento na rede local do Tribunal (On premise)

Nome da Solução: Ferramenta de Gestão de Vulnerabilidades On premises

Fornecedores: Tenable (Cotação 0834081) e Rapid7 (Cotação 0834093)

Descrição: Aquisição de software de gerenciamento de vulnerabilidades e análise dinâmica de aplicações web baseado em gerenciamento e armazenamento na rede local do tribunal, com modelo de subscrição por 60 meses ou de licença perpetua com suporte de 60 meses.

6.2. Análise de Custos Totais das Soluções de TIC Identificadas

Os custos estimados da contratação são conforme tabela abaixo.

Soluções de TIC - propostas de possíveis fornecedores/pesquisa no mercado de TIC

Item	Fornecedor	Descrição/Modelo	Quantidade Prevista	Quantidade Registrada	Valor Unitário	Valor Total
6.1.1	Comunidades	Softwares livres OpenVas e Nmap	0	0	R$ 0,00	R$ 0,00
6.1.2. - 02	Qualys (on cloud)	Licenciamento de plataforma de gestão de vulnerabilidades e auditoria de	1	1	R$ 137.826,00	R$ 137.826,00

		configurações de ativos de rede, contemplando no mínimo 250 endereços IP, por 36 meses de uso e suporte do fabricante.				
6.1.2.- 03	Qualys (on cloud)	Licenciamento para solução de análise dinâmica em aplicações Web, pacote para no mínimo 5 domínios (FQDN), por 36 meses de uso e suporte do fabricante.	1	1	R$ 59.970,00	R$ 59.970,00
6.1.2. - 05	Qualys (on cloud)	Instalação e configuração.	1	1	R$ 6.890,00	R$ 6.890,00
6.1.2. -06	Qualys (on cloud)	Repasse Tecnológico com período mínimo de 20 horas.	1	1	R$ 4.500,00	R$ 4.500,00
6.1.2.-07	Qualys (on cloud)	4 Horas de Serviço Especializado.	50	50	R$ 1250,00	R$ 62.500,00
6.1.2	TOTAL Qualys (on cloud)	----------	----------	----------	----------	R$ 209.186,00
6.1.2-02	Rapid7 (on cloud)	Licenciamento de plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando no mínimo 250 endereços IP, por 36 meses de uso e suporte do fabricante.	1	1	R$ 155.375,00	R$ 155.375,00
6.1.2-03	Rapid7 (on cloud)	Licenciamento para solução de análise dinâmica em aplicações	1	1	R$ 246.600,00	R$ 246.600,00

		Web, pacote para no mínimo 5 domínios (FQDN), por 36 meses de uso e suporte do fabricante.				
6.1.2-05	Rapid7 (on cloud)	Instalação e configuração e repasse Tecnológico com período mínimo de 20 horas.	1	1	R$ 38.000,00	R$ 38.000,00
6.1.2-06	Rapid7 (on cloud)	Repasse Tecnológico com período mínimo de 20 horas.	1	1	R$ 10.000,00	R$ 10.000,00
6.1.2-07	Rapid7 (on cloud)	4 Horas de Serviço Especializado.	50	50	R$ 1000,00	R$ 50.000,00
6.1.2	TOTAL Rapid7 (on cloud)	----------	----------	----------	----------	R$ 449.975,00
6.1.2-02	Tenable (on cloud)	Licenciamento de plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando no mínimo 250 endereços IP, por 36 meses de uso e suporte do fabricante	1	1	R$ 158.250,00	R$ 158.250,00
6.1.2-03	Tenable (on cloud)	Licenciamento para solução de análise dinâmica em aplicações Web, pacote para no mínimo 5 domínios (FQDN), por 36 meses de uso e suporte do fabricante.	1	1	R$ 64.710,00	R$ 64.710,00
6.1.2-05	Tenable (on cloud)	Instalação e configuração e repasse Tecnológico com	1	1	R$ 11.322,00	R$ 11.322,00

		período mínimo de 20 horas.				
6.1.2-06	Tenable (on cloud)	Repasse Tecnológico com período mínimo de 20 horas	1	1	R$ 8.342,00	R$ 8.342,00
6.1.2-07	Tenable (on cloud)	4 Horas de Serviço Especializado.	50	50	R$ 0,00	R$ 0,00
6.1.2	TOTAL Tenable (on cloud)	----------	----------	----------	----------	R$ 242.624,00
6.1.3-02	Rapid7 (on premise)	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 do fabricante.	1	1	R$ 155.375,00	R$ 155.375,00
6.1.3-03	Rapid7 (on premise)	Licenciamento para solução de análise dinâmica em aplicações Web, pacote para no mínimo 10 domínios (FQDN), por 60 meses de uso e suporte do fabricante.	1	1	R$ 369.930,00	R$ 369.930,00
6.1.3-05	Rapid7 (on premise)	Instalação e configuração e repasse Tecnológico com período mínimo de 20 horas.	1	1	R$ 38.000,00	R$ 38.000,00
6.1.3-06	Rapid7 (on premise)	Repasse Tecnológico com período mínimo de 20 horas.	1	1	R$ 10.000,00	R$ 10.000,00
6.1.3-07	Rapid7 (on premise)	4 Horas de Serviço Especializado.	50	50	R$ 1000,00	R$ 50.000,00

6.1.3	TOTAL Rapid7 (on premise)	----------	----------	----------	----------	R$ 487.482,00
6.1.3-02	Tenable (on premise)	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 do fabricante.	1	1	R$ 215.650,96	R$ 215.650,96
6.1.3-03	Tenable (on premise)	Licenciamento para solução de análise dinâmica em aplicações Web, pacote para no mínimo 10 domínios (FQDN), por 60 meses de uso e suporte do fabricante.	1	1	R$ 0,00	R$ 0,00
6.1.3-05	Tenable (on premise)	Instalação e configuração.	1	1	R$ 11.322,00	R$ 11.322,00
6.1.3-06	Tenable (on premise)	Repasse Tecnológico com período mínimo de 20 horas	1	1	R$ 8.342,0	R$ 8.342,00
6.1.3-07	Tenable (on premise)	4 Horas de Serviço Especializado.	50	50	R$ 0,00	R$ 0,00
6.1.3	Tenable (on premise)	----------	----------	----------	----------	R$ 235.314,00

7. Justificativa da Solução Escolhida

A solução 1 baseada em Software Livre atende apenas parte da necessidade, pois a utilização desse cenário implica em não contar com suporte técnico especializado, além disso a atualização da base de vulnerabilidades e falhas não possui a mesma frequência de cenários com softwares pagos. Outro ponto desfavorável ao uso do Software Livre é que os relatórios fornecidos pela ferramenta não apresentam rastreabilidade das atividades já realizadas nos ativos e sistemas.

A solução 2 baseada em nuvem (cloud computing) apresenta facilidade de gerenciamento, valor de aquisição adequado e facilidade nas atualizações da solução que serão todas feitas pelo fabricante. Todas os requisitos de funcionalidades do projeto são atendidos por esse cenário. As soluções analisadas Qualys (VM e módulo WAS), Tenable (Tenable.io e módulo WAS) e Rapid7 (IVM e módulo IAS) conseguem fazer o gerenciamento de vulnerabilidades em ativos de tecnologia da informação além de testes em aplicações Web. Porém como os dados armazenados pela ferramenta (vulnerabilidades dos ativos de TIC) são muito sensíveis não é recomendável estarem armazenados em nuvem pública.

A solução 3 baseada em gerenciamento em rede local do tribunal (On premises) fornecida pela Tenable apresenta um valor de aquisição adequado e menor do que a Solução 2 (On cloud). Apesar de a solução 3 (On premise) trazer o trabalho de atualização para a equipe de infraestrutura de rede, ela possui um menor risco de vazamento de dados sensíveis que são as vulnerabilidades dos ativos de TIC do tribunal pois os mesmos serão armazenados na rede local do Tribunal e não em nuvem pública. Todas os requisitos de funcionalidades do projeto também são atendidos por esse cenário. As soluções analisadas Tenable (Tenable.sc) e Rapid7 (Nexpose e módulo AppSpider) conseguem fazer o gerenciamento de vulnerabilidades em ativos de tecnologia da informação além de testes em aplicações Web. Outro ponto favorável a solução 3 fornecida pela Tenable é o fato de que após o término do suporte a STIC continuará a ter acesso a ferramenta embora sem o direito de recebimento de atualizações de versão e de novas vulnerabilidades.

Sendo assim, não resta outra alternativa para o TRE no momento senão a solução 3 baseada no gerenciamento em rede local do tribunal, tendo em vista o menor preço da Solução 3 e o fato de fazer o gerenciamento de vulnerabilidades em ativos de tecnologia da informação além de testes em aplicações Web sem armazenar em nuvem pública os dados sensíveis que são as vulnerabilidades dos ativos de TIC do tribunal.

Apesar de termos escolhido a Solução 3 (On Premise) será necessário o registro da Solução 2 (On Cloud) em um outro lote distinto porque alguns tribunais eleitorais demonstraram interesse em serem participes para registro da Solução 2 (On Cloud) e outros tribunais eleitorais em serem participes para registro da Solução 3 (On Premise).

7.1. Solução Escolhida

Nome: Solução paga com gerenciamento e armazenamento na rede local do tribunal (On Premise)

Descrição: Aquisição de software de gerenciamento de vulnerabilidades e análise dinâmica de aplicações web baseado em gerenciamento e armazenamento na rede local do tribunal, com modelo de subscrição por 60 meses ou de licença perpetua com suporte de 60 meses.

Valor Estimado (baseado na melhor proposta da Tenable on premise): R$ 235.314,00 (duzentos e trinta e cinco mil trezentos e quatorze reais)

7.2. Justificativa

Com a solução escolhida será possível realizar o Gerenciamento de vulnerabilidades, mitigando riscos de ataques cibernéticos e protegendo os sistemas de tecnologia da informação da Justiça Eleitoral.

7.3. Benefícios Esperados

Gerenciamento de vulnerabilidades, mitigando riscos de ataques cibernéticos e protegendo os sistemas de tecnologia da informação da Justiça Eleitoral e Conformidade com normas de gestão de segurança da informação.

7.4. Alinhamento em relação às necessidades

A solução escolhida se alinha perfeitamente com as necessidades do negócio e com os requisitos tecnológicos.

7.5. Relação entre a demanda prevista e a quantidade dos bens e/ou serviços a serem contratados

Devido a restrições orçamentárias e tendência natural de aumento da quantidade de ativos de TIC na rede local do tribunal optamos pela modalidade de Registro de preços nos quantitativos previstos e registrados na tabela do item 6.2.

8. Necessidades de Adequação do Ambiente do Órgão

Não haverá necessidade de adequação do ambiente, tendo em vista que a contratação não alterará em nada o ambiente atualmente em uso.

Seção II - SUSTENTAÇÃO DO CONTRATO

Como não há nenhuma consideração a ser feita no tocante à estratégia de sustentação do contrato, estaremos suprimindo esta parte.

Seção III - ESTRATÉGIA PARA A CONTRATAÇÃO

9. Natureza do objeto

Trata-se de uma licença de software, cujo uso é comum a diversas instituições da Administração Pública Federal, sendo assim um padrão de mercado.

10. Parcelamento do objeto

O objeto pode ser dividido pelos itens que compõem a solução.

11. Adjudicação do objeto

A adjudicação do objeto pode ser feito por lote, que podem ser fornecidos por diferentes empresas, tendo em vista que os itens do lote compõem uma solução global, interdependente e indivisível.

12. Modalidade e tipo de licitação

Após realização dos estudos técnicos chegou-se aos seguintes quantitativos de material, descrito por meio da tabela do item 6.1, a serem licitados em dois lotes único (por se tratar de soluções distintas e indivisíveis) e através do sistema de Registro de Preços (por restrições orçamentárias e por não ser possível precisar de início o quantitativo a ser pedido durante a vigência da ata):

13. Classificação e indicação orçamentária

Orçamento ordinário da COINF para o exercício de 2020, APOIO TÉCNICO E OPERACIONAL DE TIC e COMUNICAÇÃO E REDES DE DADOS

14. Vigência da prestação de serviço

A vigência dos itens registrados será de 60 meses, a depender da garantia explicitada para o item em questão.

15. Equipe de Apoio à Contratação

A equipe de apoio à contratação será composta pela mesma equipe do presente estudo preliminar constante do item 02 deste documento.

RODRIGO PINTO DE CARVALHO

COINF

EUZEBIO RODRIGUES CARDOSO JUNIOR

SEAU

RUBENS ANTONIO PINTO SOARES

SEPD