TRIBUNAL SUPERIOR ELEITORAL

ESTUDOS PRELIMINARES DA CONTRATAÇÃO

I – Apresente a necessidade a ser atendida:

Realizar a Gestão de Vulnerabilidades em Ativos de Tecnologia da Informação

II – Indique o público-alvo (unidades orgânicas, autoridades, servidores, outros) da contratação:

A Gestão de Vulnerabilidades em Ativos de Tecnologia da Informação é uma atividade a ser executada pela Secretaria de Tecnologia da Informação. Tais ativos, entretanto, suportam todas os sistemas e aplicações utilizadas pelas diversas unidades organizacionais do tribunal.

III – Indique a(s) consequência(s), caso não haja atendimento da necessidade:

Vulnerabilidades em Ativos de Tecnologia da Informação representam as fraquezas existentes nesses ativos que podem ser exploradas por atacantes para a realização de ataques cibernéticos. A Gestão de Vulnerabilidades é uma disciplina que permite a identificação, classificação em termos de severidade, e priorização no tratamento de vulnerabilidades. A não realização da Gestão de Vulnerabilidades mantém alto o nível de risco do ambiente de Tecnologia da Informação, expondo os sistemas e aplicações do tribunal a ataques, facilitando a ocorrência de incidentes de segurança tais como divulgação não autorizada de informações sensíveis, adulteração de informações, etc., o que pode causar prejuízos materiais e de imagem ao tribunal.

IV – Indique o alinhamento da necessidade ao Planejamento Estratégico do TSE:

Conforme indicado no Documento de Oficialização de Demandas, a aquisição está alinhada ao Planejamento Estratégico da seguinte forma:

Objetivo Estratégico Institucional:

OE11 – Garantir a eficiência na prestação dos serviços de tecnologia da informação e comunicação

Planejamento Estratégico de TI

OETIC 7–Aprimorar as práticas e os controles de segurança da informação utilizados no desenvolvimento e na operação de serviços e de soluções de TI

IN07.01Implementar iniciativas que visam ao aprimoramento das práticas e dos controles de segurança da informação utilizados no desenvolvimento e na operação de serviços e soluções de TIC providas pela STI.

V – Indique o resultado da pesquisa de mercado feita para identificação das diferentes soluções que possam atender às necessidades explicitadas:

	Solução identificada	Detalhamento das Soluções
1ª	Soluções disponibilizadas de forma gratuita	Ferramentas disponibilizadas sob a modalidade de software livres (código aberto) ou gratuitamente, como os softwares OpenVas e Nmap
2ª	Solução comercial com gerenciamento e armazenamento na nuvem (On Cloud)	Aquisição de software de gerenciamento de vulnerabilidades e análise dinâmica de aplicações web baseado em nuvem, com modelo de subscrição por tempo determinado

3ª	Solução comercial com gerenciamento e armazenamento na rede local do Tribunal (On premise)	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 tempo determinado, ou de licença perpetua com suporte técnico por tempo determinado

A pesquisa de preços referente às opções comerciais encontra-se no documento SEI 1441027.

Faz-se importante destacar que trata-se de solução de prateleira, com produtos similares desenvolvidos por diferentes fabricantes, usualmente disponível no mercado para contratação por órgãos públicos e entidades privadas, razão pela qual não é cabível a indicação, para cada solução, dos órgãos públicos ou entidades que as tenham adotado.

Quanto à quantidade de soluções comerciais, observamos que a quantidade de fabricantes é pequena, que, entretanto, contam com uma rede razoável de revendas no mercado nacional. As especificações técnicas procuraram refletir as necessidades técnicas do tribunal, sem a inserção de exigências injustificadas. Questões de segurança, entretanto, foram consideradas, e serão detalhadas no trecho referente à escolha da solução.

Vantagens e Desvantagens de cada solução

Opção nº 1, "Soluções disponibilizadas de forma gratuita":

Vantagens:

Essas soluções não apresentam custo de aquisição, uma vez que são disponibilizada de forma gratuita por seus fabricantes, ou ainda no formato de código aberto, onde toda a comunidade pode ter acesso ao código fonte dos diversos programas que as compõem.

Desvantagens:

Atendem apenas parte da necessidade, uma vez que tais soluções não contam com suporte técnico especializado, sua frequência de atualização da base de vulnerabilidades é inferior às alternativas comerciais, e não dispõem de funções importantes como a existência de fontes de inteligência sobre ameaças (*Threat Intelligence*) e funcionalidades avançadas de priorização da mitigação de vulnerabilidades. Outro ponto desfavorável com relação a esta opção é que os relatórios fornecidos não apresentam rastreabilidade das atividades já realizadas nos ativos e sistemas.

Obs: Faz-se importante destacar que o tribunal já se utiliza da solução OpenVAS, uma das representantes das soluções gratuitas, e a existência dessas limitações é a motivação para a realização da presente aquisição.

Opção nº 2, "Solução comercial com gerenciamento e armazenamento na nuvem (On Cloud)":

Vantagens:

Atendem todos os requisitos de funcionalidades descritas na especificação da solução, fornecendo todas as funcionalidades apontadas como desvantagens relacionadas à Opção 1.

Adicionalmente, apresenta facilidade de gerenciamento, uma vez que o componente central da solução é provido em ambiente de nuvem pública, não sendo necessário o esforço, por parte do tribunal, para instalação, configuração e eventuais atualizações do ambiente, uma vez que todas essas tarefas são de responsabilidade do próprio fabricante, em função da natureza da solução.

Desvantagens:

Como pontos negativos apontamos o fato de os dados armazenados pela ferramenta (vulnerabilidades dos ativos de TIC), que são de natureza sensível, serem armazenados em nuvem pública, e o fato de que, ao final do período de subscrição, o acesso à ferramenta é completamente indisponibilizado ao tribunal, inviabilizando até mesmo as consultas às análises de vulnerabilidades previamente conduzidas.

A opção nº 3, "Solução comercial com gerenciamento e armazenamento na rede local do Tribunal (On premise)":

Vantagens:

Todos os requisitos de funcionalidades do projeto também são atendidos por esse cenário.

Apresenta um menor risco de vazamento de dados sensíveis que são as vulnerabilidades dos ativos de TIC, pois os mesmos serão armazenados localmente e não em nuvem pública.

Outro ponto favorável é o fato de que após o término do período de suporte contratado, o tribunal continuará a ter acesso à ferramenta, embora sem o direito de recebimento de atualizações de versão e de novas vulnerabilidades. Ainda que tal acesso não seja o mais adequado para a realização de novas análises de vulnerabilidades, em razão de sua desatualização, todas as análises previamente realizadas permanecem acessíveis, facilitando a tarefa de correção dos problemas encontrados.

Desvantagens:

Traz para o tribunal o esforço de atualização da solução (por meio de mão de obra própria ou de previsão contratual para execução por parte da empresa contratada), uma vez que a mesma passa a estar instalada em nosso próprio ambiente de TI.

Outros órgãos públicos que adotaram soluções de Gestão de Vulnerabilidades

Nas pesquisas que realizamos identificamos os seguintes órgãos públicos como exemplos de entidades que já realizaram a aquisição de soluções de Gestão de Vulnerabilidades:

- Banrisul (Pregão Eletrônico nº 509/2019 - documento 1472768): Solução de Gestão de Vulnerabilidades na modalidade de instalação local
- Conselho da Justiça Federal (Pregão Eletrônico nº 1/2020 - documento 1472778): Gestão de Vulnerabilidades como parte de um conjunto de Serviços Gerenciados de Segurança da Informação
- INEP (Termo de Referência - Processo 23036.001606/2017-15 - documento 1472784): Gestão de Vulnerabilidades na modalidade de instalação local, como parte de um conjunto de Serviços Gerenciados de Segurança
- Superior Tribunal de Justiça (Contrato STJ 86/2018 - documento 1472790): Solução de Gestão de Vulnerabilidades na modalidade de instalação local
- Tribunal Regional Eleitoral do Paraná (ARP 3/2020 - documento 1472800): Solução de Gestão de Vulnerabilidades na modalidade nuvem pública.

VI – Indique a descrição completa da solução que, por entendimento do(s) signatário(s) deste documento, melhor atenderá à necessidade especificada neste documento:

Especificação Técnica da Solução

1. Deve estar licenciada de tal forma que estejam inclusas todas as funcionalidades para realizar varreduras de vulnerabilidades, avaliação de configuração e conformidade (*baseline e compliance*), indícios e padrões de códigos maliciosos conhecidos (malware).
2. Deve ser licenciada para um número ilimitado de scanners (prevendo redundância);
3. Todas as licenças de uso de software devem ser registradas no site do fabricante, na data da entrega, em nome da Contratante;
4. Deve possuir recurso de varredura ativa, onde o scanner comunica-se com os alvos (ativos) através da rede;
5. Deve permitir mecanismo de varredura baseado em inferência com técnicas de varredura não intrusivas;
6. Deve suportar varreduras de dispositivos de *IoT* (Internet das Coisas);
7. Deve ser capaz de identificar no mínimo 50.000 *CVEs* (*Common Vulnerabilities and Exposures*);
8. 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;
9. Deve atribuir a todas as vulnerabilidades uma severidade baseada no *CVSSv3 score*;
10. Deve calcular a criticidade com base nos dados agregados e consolidados do ativo, dados de segurança, sistema e conformidade, bem como hierarquias e prioridades;
11. Deve fornecer criptografia de ponta a ponta (envolvendo coleta, transmissão e armazenamento) dos dados referentes aos ativos avaliados, vulnerabilidades identificadas, e outras informações sobre o ambiente do tribunal;
12. Deve possuir a capacidade de armazenar informações dos ativos descobertos no ambiente;
13. Deve possuir um sistema de busca de informações de um determinado ativo com no mínimo as seguintes características;
    1. Por sistema operacional;
    2. Por um determinado software instalado;
    3. Por Ativos impactados por uma determinada vulnerabilidade.
14. Deve possuir suporte para a adição de detecções personalizadas usando o *OVAL (Open Vulnerability Assessment Language)*;
15. Deve permitir aceitar o risco de uma determinada vulnerabilidade encontrada no ambiente;
16. Deve possibilitar alterar a criticidade de determinada vulnerabilidade de forma manual;
17. Deve possuir um sistema de pontuação e priorização das vulnerabilidades;
18. Deve ser capaz de aplicar algoritmos de aprendizagem de máquina *(machine learning*) para analisar as características relacionadas a vulnerabilidades;
19. O sistema de pontuação e priorização de vulnerabilidades deve avaliar no mínimo as seguintes características:
    1. *CVSSv3 Impact Score*;
    2. Idade da Vulnerabilidade;
    3. Se existe ameaça ou *exploit* publicados que explorem a vulnerabilidade;
    4. Número de produtos afetados pela vulnerabilidade;
20. Deve ser capaz de fazer a correlação em tempo real de ameaças ativas contra vulnerabilidades encontradas, incluindo *feeds* de inteligência de ameaças ao vivo;
21. Deve possuir uma API para automação de processos e integração com aplicações terceiras permitindo, no mínimo, a extração de dados para carga em soluções de *SIEM (Security Information and Event Management)*;
22. Deve possuir uma API para automação de processos e integração com aplicações ITSM *(Information Technology Service Management)* do órgão para a abertura de chamados técnicos referentes às vulnerabilidades encontradas, permitindo o agrupamento no chamado por ações corretivas;
23. Deve permitir a instalação de agentes em estações de trabalho e servidores, para varredura diretamente no sistema operacional;
24. Deve possuir conectores para, no mínimo, as seguintes plataformas de serviços em nuvem:
    1. Amazon Web Service (AWS);

2. Microsoft Azure;
3. Google Cloud Platform.

25. Deve possuir recurso de monitoria passiva do tráfego de rede para identificação de anomalias, novos dispositivos e desvios de padrões observados;
26. Deve ser licenciada para o uso ilimitado de sensores passivos de rede para realizar o monitoramento em tempo real;
27. Deve possuir sensores, no mínimo, com as seguintes funcionalidades:
    1. Execução de verificação completa do sistema (rede), adequada para qualquer ativo;
    2. Verificação sem recomendações da rede, para que se possa personalizar totalmente as configurações da verificação;
    3. Autenticação de ativos e enumeração de atualizações ausentes;
    4. Execução de varredura simples para descobrir ativos em operação e portas TCP/UDP abertas;
    5. Utilização de um scanner para verificar aplicativos da web;
    6. Avaliação de dispositivos móveis
    7. Auditoria de configuração de serviços em nuvem de terceiros;
    8. Auditoria de configuração dos gerenciadores de dispositivos móveis;
    9. Auditoria de configuração dos dispositivos de rede;
    10. Auditoria de configurações do sistema em relação a uma linha de base conhecida;
    11. Detecção de desvio de segurança Intel AMT;
    12. Verificação de malware nos sistemas Windows e Unix;
28. Deve ser possível determinar em tempo real quais portas de serviços (UDP/TCP) estão abertas em determinado ativo;
29. Deve ser capaz de realizar em tempo real a descoberta de novos ativos para no minímo:
    1. Bancos de dados;
    2. Hypervisors (no mímino VMWare ESX/ESXi);
    3. Dispositivos móveis;
    4. Dispositivos de rede;
    5. Endpoints;
    6. Aplicações;
30. Deve ser capaz de, em tempo real, detectar logins e downloads de arquivos em um compartilhamento de rede;
31. Permitir identificar vulnerabilidades associadas a servidores SQL no tráfego de rede;
32. Deve possuir interface para integração com as principais soluções de *SIEM (Security Information and Event Management)* de mercado, tais como IBM QRadar, Microfocus ArcSight e Splunk;
33. 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.
34. A atualização das bases de conhecimento sobre vulnerabilidades e ameaças deve ocorrer diariamente e sem interrupção dos serviços.
35. Configuração de segurança e acesso à gerência da solução:
    1. Todos os dados armazenados nos servidores da solução devem ser criptografados e possuir logs de acesso;
    2. As conexões para o envio de dados devem ser estabelecidas utilizando-se no mínimo o algoritmo TLS 1.2 de chave 2048 bits;
    3. Os dados em trânsito devem ser criptografados ao menos com o algoritmo AES-128 bits;
    4. As funções de hash devem usar ao menos o algoritmo SHA-256;
    5. Os dados armazenados devem ser criptografados ao menos com o algoritmo AES-256 bits;
    6. Será aceito como comprovação dos critérios de criptografia a publicação em site do fabricante ou declaração do próprio fabricante;

7. Somente servidores da Contratante ou pessoa por ela autorizada poderão ter acesso aos dados da solução;
8. A solução deve permitir a criação de, no mínimo, 20 contas para gerência e acesso aos relatórios, sem custo adicional;
9. A empresa contratada não deverá ter acesso à rede interna da Contratante e, em caso de opção pela utilização da solução hospedada em nuvem, todo tráfego de dados de saída deverá ser iniciado pelos scanners instalados no ambiente de TI da própria Contratada.

36. Deve ser capaz de produzir relatórios nos seguintes formatos: PDF, CSV, HTML e no formato de texto que poderá ser DOCX ou RTF;
    1. Deve ser capaz de executar relatórios periódicos de acordo com a frequência estabelecida pelo administrador, bem como a geração de relatórios sob demanda;
    2. A solução deve possibilitar a criação de relatórios baseados na seleção de ativos, permitindo inclusive a seleção de todos os ativos existentes;
    3. Deve suportar a criação de relatórios criptografados (protegidos por senha configurável) ;
    4. Deve suportar o envio automático de relatórios para destinatários específicos;
    5. Deve ser possível definir a frequência na geração dos relatórios para no mínimo: Diário, Mensal, Semanal e Anual;
    6. Permitir especificar níveis de permissão nos relatórios para usuários e grupos específicos;
    7. Deve fornecer relatórios do tipo *"scorecard"* para as partes interessadas da empresa;
    8. Deve fornecer relatórios de correções aplicadas, classificados pelos seguintes critérios: grupo de ativos, usuários e vulnerabilidades;
37. A solução deve possuir ou permitir a criação de relatórios com as seguintes informações:
    1. Ativos verificados sem credenciais;
    2. Vulnerabilidades mais críticas;
    3. Ativos mais infectados por Malwares;
    4. Ativos exploráveis por Malwares;
    5. Total de vulnerabilidades que podem ser exploradas por meio da plataforma Metasploit;
    6. Vulnerabilidades críticas e exploráveis;
    7. Ativos com vulnerabilidades que podem ser exploradas;
38. A solução deve possuir dashboards customizáveis onde o administrador pode criar, editar ou remover painéis de acordo com a necessidade;
39. A solução deve ser capaz de realizar o inventário básico de todos os ativos da rede local e publicados na Internet, sem limites de endereços IP, coletando ao menos as informações sobre nome do ativo, endereço IP e Sistema Operacional.
40. Deve permitir a configuração de vários painéis e widgets;
41. Deve ser capaz de medir e reportar ameaças;
42. Deve ser capaz de visualizar ameaças críticas ao ambiente monitorado;
43. 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
44. A plataforma de software deve suportar vários mecanismos de varredura distribuídos em diferentes localidades e regiões e gerenciar todos por uma console central;
45. 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;
46. A plataforma de software deve permitir o monitoramento através de agentes instalados, até o limite de licenças adquiridas, para varredura diretamente no sistema operacional.
47. 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.

48. 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;
49. 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;
50. A plataforma de software deve ser configurável para permitir a otimização das parametrizações de varredura;
51. 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;
52. A plataforma de software deve fornecer a capacidade de escalar privilégios nos destinos, do acesso de usuário padrão até acesso de sistema ou administrativo;
53. A plataforma de software deve ser capaz de realizar pesquisas de dados confidenciais.
54. 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;
55. 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;
56. A solução de análise deve ser capaz de analisar, testar e reportar falhas de segurança em aplicações Web;
57. A solução de análise deverá ser capaz de executar varreduras em sistemas Web através de seus endereços IP ou FQDN (DNS);
58. A solução de análise deve ser capaz de identificar vulnerabilidades de divulgação de dados, como vazamento de informações de identificação pessoal;
59. Para varreduras do tipo extensas e detalhadas, deve varrer e auditar no mínimo os seguintes elementos:
    1. *Cookies, Headers*, Formulários e *Links*;
    2. Nomes e valores de parâmetros da aplicação;
    3. Elementos *JSON* e *XML*;
    4. Elementos *DOM*;
60. Deverá também permitir a execução da função *crawler*, que consiste na navegação para descoberta das *URLs* existentes na aplicação;
61. A solução de análise deve suportar a integração com os softwares de automação de testes para permitir sequências de autenticação complexas;
62. A solução de análise deve ser capaz de realizar testes/varreduras em aplicações separadas, simultaneamente limitadas ao número de licenças;
63. Suporte a ferramentas para construção de requisições e análise de respostas de aplicações *WEB*, *API's* e *WebServices*, tais como *Postman Collections*;
64. A solução de análise deve oferecer suporte à capacidade de testar novamente a vulnerabilidade específica que foi detectada anteriormente no aplicativo *Web*;
65. Deve ser capaz de utilizar scripts customizados de *crawling* com parâmetros definidos pelo usuário;
66. Deve ser capaz de excluir determinadas *URLs* da varredura através de expressões regulares;
67. Deve ser capaz de excluir determinados tipos de arquivos através de suas extensões;
68. Deve ser capaz de instituir no mínimo os seguintes limites:
    1. Número máximo de *URLs* para *crawling* e navegação;
    2. Número máximo de diretórios para varreduras;
    3. Número máximo de elementos *DOM*;
    4. Tamanho máximo de respostas;
    5. Tempo máximo para a varredura;
    6. Número máximo de conexões HTTP(S) ao servidor hospedando a aplicação *Web*;
    7. Número máximo de requisições HTTP(S) por segundo;

69. Deve ser capaz de agendar a varredura e determinar sua frequência entre uma única vez, diária, semanal, mensal e anual;
70. Deve suportar o envio de notificações por email;
71. Deverá ser compatível com avaliação de *web services REST e SOAP*;
72. A solução de análise deve suportar os seguintes esquemas de autenticação:
    1. Autenticação Básica (*Digest*);
    2. *NTLM*;
    3. Autenticação de *Cookies*;
73. Deve ser capaz de importar scripts de autenticação previamente configurados pelo usuário;
74. 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;
75. Os resultados devem ser apresentados agregados por vulnerabilidades ou por aplicações;
76. Para cada vulnerabilidade encontrada, devem ser exibidos detalhes e evidências;
77. Cada vulnerabilidade encontrada deve conter também soluções propostas para mitigação ou remediação;
78. Serviço de Detecção de Malware:
    1. Deve utilizar a plataforma de gerenciamento de vulnerabilidades existente;
    2. Deve permitir visualizar o acompanhamento das atividades de verificação, páginas infectadas e tendências de infecção por malware;
    3. 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.
79. A solução deve ser capaz de realizar varreduras nos seguintes componentes/aplicações:
    1. WordPress;
    2. IIS 6.x e IIS 10.x;
    3. ASP 6;
    4. .NET 2;
    5. Apache HTTPD 2.2.x e 2.4.x;
    6. Tomcat 6.x, 7.x, 8.x e superiores;
    7. Jetty 8 e superiores;
    8. Nginx;
    9. PHP 5.3.x, 5.4.x, 5.6.x, 7.0.x e 7.1.x e superiores;
    10. Java 1.5, 1.6, 1.7 e 1.8 e superiores;
    11. Jboss 4.x e 7.x e superiores;
    12. WildFly 8 e 10 e superiores;
    13. Plone 2.5.x e 5.2.1.41.x e superiores;
    14. Zope;
    15. Python 2.4.4 e superiores;
    16. J2EE;
    17. Ansible;
    18. Joomla;
    19. Moodle;
    20. Docker Conteiner;
    21. ELK;
    22. GIT;
    23. Grafana; e
    24. Redmine.

Obs: A especificação técnica prevê compatibilidade com plataformas de nuvem pública (Amazon AWS, Microsoft Azure e Google Cloud) e com alguns produtos disponibilizados sob a modalidade de software livre (Joomla e Wordpress) que, embora não sejam atualmente utilizados pelo TSE, são produtos padrão de mercado, que podem vir a ser utilizados pelo tribunal em virtude de novos projetos. Tal previsão de compatibilidade tem o condão de evitar a aquisição de um produto de Gestão de Vulnerabilidades que facilmente se torne incompatível com o parque de Tecnologia da Informação do tribunal.

Serviços de Instalação e Configuração

A Contratada deverá instalar a solução e configurá-la para a utilização por parte do Tribunal Superior Eleitoral.

Deverá ainda realizar as atualizações da solução, conforme liberação de novas versões por parte do fabricante.

Requisitos de Capacitação

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

Requisitos Temporais

Prazos

A Contratada terá 15 (quinze) dias corridos, contados da assinatura do contrato, para fornecer os softwares ou as subscrições contratadas;

A Contratada terá 15 (quinze) dias corridos, contados a partir do fornecimento, para realizar a instalação e configuração da solução.

Suporte e garantia

O Suporte remoto por parte do fabricante, bem como a garantia de atualização do software devem ser de, no mínimo, 36 (trinta e seis) meses.

Requisitos de Segurança

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 Superior Eleitoral aos quais tiver acesso em decorrência do objeto da presente contratação, ficando terminantemente proibida de fazer uso ou revelação destes sob qualquer justificativa;

O Tribunal Superior Eleitoral terá propriedade sobre todos os documentos e procedimentos operacionais produzidos no escopo da presente contratação;

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

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.

Requisitos Sociais, Ambientais e culturais

- A solução deve ser disponibilizada para instalação, e seus manuais devem ser disponibilizados para acesso, de forma *on-line*, sem o uso de dispositivos físicos;

- A contratada não deve possuir inscrição no cadastro de empregadores flagrados explorando trabalhadores em condições análogas às de escravo;
- A contratada, ou seus dirigentes, não deve ter sido condenada por infringir as leis de combate à discriminação de raça ou de gênero, ao trabalho infantil e ao trabalho escravo;
- Apresentação do Programa de Controle Médico de Saúde Ocupacional (PCMSO);
- Apresentação do Programa de Prevenção de Riscos Ambientais (PPRA);
- Atendimento ao art. 93 da Lei nº 8.213/91

Transição Contratual

Não é necessária a previsão de atividades de transição contratual. Não há contrato anterior para o mesmo objeto, e o objeto é o fornecimento de uma solução para utilização por parte do tribunal sem a execução de serviços associados por parte da Contratada, à exceção da instalação e configuração da solução, e do suporte remoto por parte do fabricante para a resolução de eventuais problemas apresentados pelo produto e para o esclarecimento de dúvidas de utilização.

Benefícios Diretos e Indiretos pretendidos com a contratação

Conforme informado no Documento de Oficialização de Demanda, os Resultados a Serem Alcançados, que trazem em si os benefícios pretendidos com a contratação, são os seguintes:

- Identificação das vulnerabilidades das soluções de TIC utilizadas pelo TSE.

- Redução do nível de risco do ambiente de TIC por meio da correção das vulnerabilidades identificadas;

Necessidade de serviços de manutenção

A necessidade de serviços de manutenção já se encontra prevista no item "Serviços de Instalação e Configuração", que prevê a necessidade de atualizações do produto por ocasião da liberação de versões por parte do fabricante, e na exigência de suporte técnico remoto pelo fabricante.

Formação e experiência profissional da equipe que realizará os serviços

A equipe que realizará os serviços de instalação, configuração e atualização de versões deverá possuir certificação emitida pelo fabricante, em modalidade que ateste que a equipe está qualificada para a realização de tais serviços.

Seleção da solução

A opção nº 1 representa o tipo de solução que já se encontra em utilização no tribunal atualmente, e, como suas limitações são o motivo que enseja a contratação ora almejada, é uma opção naturalmente descartada.

Com relação ao nível de segurança associado às opções nº 2 e nº 3, em razão da diferença entre a hospedagem da solução em nuvem pública ou no próprio ambiente de TI do tribunal, gostaríamos de destacar as recomendações constantes da Norma Complementar nº 14/IN01 do Departamento de Segurança da Informação e Comunicações (DSIC), subordinado ao Gabinete de Segurança Institucional da Presidência da República, que diz o seguinte:

> *"5.2.2 Informação sigilosa: como regra geral, deve ser evitado o tratamento em ambiente de computação em nuvem, conforme disposições a seguir:*
>
> *5.2.2.1. Informação classificada: é vedado o tratamento em ambiente de computação em nuvem;*
>
> *5.2.2.2. Conhecimento e informação contida em material de acesso restrito: é vedado o tratamento em ambiente de computação em nuvem;*

....

5.3 Deve ser assegurado que dados, metadados, informações e conhecimento, produzidos ou custodiados por órgão ou entidade da APF, bem como suas cópias de segurança, residam em território brasileiro;"

Observa-se que existe a vedação do armazenamento de informação classificada ou de acesso restrito em ambientes de nuvem, além da recomendação de que os dados produzidos ou custodiados por órgão ou entidade da APF residam em território brasileiro.

Muito embora as informações referentes às vulnerabilidades de ativos de TI não tenham sido formalmente classificadas como sigilosas ou de acesso restrito, podemos afirmar que são informações que devem ser de conhecimento de um grupo restrito de profissionais, responsáveis pelo tratamento de risco e pelas configurações de segurança do ambiente de TI do tribunal. Adotando-se tais vedações como boa prática de segurança no tratamento de informações sobre vulnerabilidades conhecidas em ativos de TI do tribunal, temos que seria ao menos recomendado seu armazenamento em ambiente interno.

Adicionalmente, as soluções hospedadas em nuvem, de acordo com a pesquisa de mercado realizada, ainda não oferecem a opção de hospedagem em ambiente de nuvem localizado em território brasileiro.

Destacamos ainda que a pesquisa de preços disponibilizada no documento 1441027 evidencia que não há grande disparidade entre os preços de ambos os tipos de solução.

Sendo assim, a alternativa selecionada é a opção nº 3, "Solução comercial com gerenciamento e armazenamento na rede local do Tribunal (On premise)", tendo em vista seu o menor preço e sua maior segurança quanto à confidencialidade das informações sobre os ativos de TI e suas vulnerabilidades.

Com relação ao prazo de licenciamento, indicamos o prazo de 36 meses, ainda que seu custo relativo, calculado por mês, seja superior ao custo do prazo de 60 meses. Tal opção se dá em função da dinamicidade das mudanças que ocorrem no cenário de tecnologia da informação, de forma tal que, após 36 meses de utilização do produto, seja recomendável uma nova avaliação de mercado para determinar as especificações técnicas mas adequadas às necessidades do tribunal.

VII – Indique o(s) estudo(s) realizado(s) ou o(s) critério(s) adotado(s) para definir o cálculo e a quantidade da necessidade:

O licenciamento das soluções de gestão de vulnerabilidades está diretamente relacionado à quantidade de endereços IP serão monitorados. Como regra geral podemos afirmar que cada Ativo de Tecnologia da Informação possui um endereço IP a ele associado. Há algumas exceções, em que um determinado ativo pode ter mais de um endereço IP utilizado para finalidades distintas, porém é uma situação que ocorre em poucos ativos que, mesmo assim, podem ter suas vulnerabilidades gerenciadas a partir de um único endereço IP.

Já para a análise dinâmica de vulnerabilidades de aplicações WEB, as soluções apresentadas estão vinculadas aos endereços Web das aplicações (endereço digitado no navegador web para acesso a uma determinada aplicação), independentemente do quantitativo de instâncias ou servidores em que essas aplicações estejam sendo executadas. Para a estimativa de aplicações a serem monitoradas, contabilizamos apenas as aplicações disponibilizadas na Internet, por serem as mais vulneráveis a ataques.

A partir das observações acima, elaboramos os seguintes quadros, detalhando as quantidades de ativos de TI e de Aplicações executadas no ambiente do TSE

Quadro 1 – Ativos de TI

Tipo de ativo	**Quantidade**
Máquinas virtuais (VM)	800
Roteadores	8
Switch de rede primário (núcleo da rede)	3
Switch de rede secundário (camada de distribuição)	12
Switch de rede terciário (camada de acesso)	31
Balanceador de links de internet	4
Storages (equipamentos para armazenamento de dados)	2
TOTAL	**860**

Obs: Informações extraídas das consoles de gerenciamentos dos ambientes de TI do tribunal.

Quadro 2 – Aplicações disponibilizadas na Internet

Aplicação	**Ambiente**
api-migra-ccontrato-dev.tse.jus.b	Desenvolvimento
apps-desenvolvimento.tse.jus.br	Desenvolvimento
justifica-dsv.tse.jus.br	Desenvolvimento
api-services-hmg.tse.jus.br	Homologação
autentica-hmg.tse.jus.br	Homologação
candex-api-simulado.tse.jus.br	Homologação
jet-homologacao.tse.jus.br	Homologação
login-hmg.tse.jus.br	Homologação
pjehmg.tse.jus.br	Homologação
pjezona-hmg.tse.jus.br	Homologação
acoeseducacionais.tse.jus.br	Produção
agencia.tse.jus.br	Produção
agenciaje.tse.jus.br	Produção
akira.tse.jus.br	Produção
api.tse.jus.br	Produção
api-justifica.tse.jus.br	Produção
api-migra-ccontrato.tse.jus.br	Produção

api-services.tse.jus.br	Produção
apps.tse.jus.br	Produção
appsinfovia01.tse.jus.br	Produção
appsinter.tse.jus.br	Produção
appspjetse03.tse.jus.br	Produção
arquivos.tse.jus.br	Produção
autentica.tse.jus.br	Produção
biblioteca.tse.jus.br	Produção
bibliotecadigital.tse.jus.br	Produção
bioex.tse.jus.br	Produção
candex-api-oficial.tse.jus.br	Produção
candex-atualizador.tse.jus.br	Produção
cdn.tse.jus.br	Produção
chimera.tse.jus.br	Produção
consultapublicapje.tse.jus.br	Produção
coyote.tse.jus.br	Produção
coyote-api.tse.jus.br	Produção
credenciamento.tse.jus.br	Produção
democraciatododia.tse.jus.br	Produção

dft.tse.jus.br	Produção
divulga.tse.jus.br	Produção
divulgacandcontas.tse.jus.br	Produção
divulgacao-resultados.tse.jus.br	Produção
divulgaspca.tse.jus.br	Produção
dje-consulta.tse.jus.br	Produção
dni.tse.jus.br	Produção
download.tse.jus.br	Produção
eadeje.tse.jus.br	Produção
educacao.tse.jus.br	Produção
english.tse.jus.br	Produção
filia-consulta.tse.jus.br	Produção
filia-externo.tse.jus.br	Produção
filiaweb.tse.jus.br	Produção
financiamentocoletivo.tse.jus.br	Produção
fiscalizaje.tse.jus.br	Produção
gel.tse.jus.br	Produção
gsti.tse.jus.br	Produção
horus.tse.jus.br	Produção

idc.tse.jus.br	Produção
inter01.tse.jus.br	Produção
inter02.tse.jus.br	Produção
inter03.tse.jus.br	Produção
inter04.tse.jus.br	Produção
investigador-tps.tse.jus.br	Produção
jet.tse.jus.br	Produção
justifica.tse.jus.br	Produção
luna.tse.jus.br	Produção
mimic.tse.jus.br	Produção
miss.tse.jus.br	Produção
molly.tse.jus.br	Produção
mural-consulta.tse.jus.br	Produção
niagara.tse.jus.br	Produção
nova.tse.jus.br	Produção
orion.tse.jus.br	Produção
pardal.tse.jus.br	Produção
pesqele.tse.jus.br	Produção
phoenix.tse.jus.br	Produção

pje.tse.jus.br	Produção
pje1g.tse.jus.br	Produção
pje1g-ead.tse.jus.br	Produção
pje2advo.tse.jus.br	Produção
pje2-advo.tse.jus.br	Produção
pje3g-ead.tse.jus.br	Produção
pjefrontend.tse.jus.br	Produção
pjefrontend-ead.tse.jus.br	Produção
qrcodenobu.tse.jus.br	Produção
reje.tse.jus.br	Produção
sacexterno.tse.jus.br	Produção
schemas.tse.jus.br	Produção
sedesc1-jud-01.tse.jus.br	Produção
seer.tse.jus.br	Produção
servicedesk.tse.jus.br	Produção
servicos.tse.jus.br	Produção
servicosdeti.tse.jus.br	Produção
sessao.tse.jus.br	Produção
sge.tse.jus.br	Produção

sherlock.tse.jus.br	Produção
sico-consulta-web.tse.jus.br	Produção
simba.tse.jus.br	Produção
sintse.tse.jus.br	Produção
sle.tse.jus.br	Produção
spcadownload.tse.jus.br	Produção
spce2010.tse.jus.br	Produção
spcedownload.tse.jus.br	Produção
spceenvio.tse.jus.br	Produção
sulu.tse.jus.br	Produção
temasselecionados.tse.jus.br	Produção
testlink-fabrica.tse.jus.br	Produção
vpn.tse.jus.br	Produção
www.tse.jus.br	Produção
zodiac4.tse.jus.br	Produção
TOTAIS	
Aplicações em Produção	98
Aplicações em Homologação	7
Aplicações em Desenvolvimento	3

Obs: Informações extraídas do ambiente de gerenciamento de aplicações disponibilizadas para a Internet do tribunal. A aquisição pretendida terá como alvo apenas as aplicações disponibilizadas para a Internet em ambiente de produção, equivalente, portanto, a 98 aplicações. É importante observar que este número de aplicações pode variar ao longo do tempo, a depender do desenvolvimento e publicação de novas aplicações, ou do encerramento do ciclo de vida de aplicações ora em produção.

VIII – Indique se a solução eleita é divisível ou não, levando em consideração o mercado que a fornece:

A solução não é divisível, uma vez que é composta por elementos interdependentes, administrados coletivamente por uma única console central de gerenciamento.

IX – Indique, entre outras, as restrições internas de caráter técnico, operacional, regulamentar, financeiro e orçamentário, que possam dificultar a implementação da solução eleita:

A principal restrição que se pode apontar para a implementação da solução eleita é a disponibilidade de pessoal para a sua correta utilização.

Entretanto, tal restrição tende a ser minimizada por meio da definição de normas e procedimentos que disciplinem a realização de Gestão de Vulnerabilidades, atividade esta que já está sendo realizada por meio do projeto "CIS Controls – Fase 1" (Processo SEI n. 2019.00.000011504-4), que, dentre seus produtos, já apresentou minuta de norma de Gestão de Vulnerabilidades, devidamente aprovada pela Comissão Técnica de Tecnologia da Informação (CTTI) e encaminhada à Comissão de Segurança da Informação (CSI) para a mesma finalidade.

X – Indique o valor estimado para a contratação:

De acordo com o Item VII deste ETP, o TSE dispõe de 860 ativos de rede, entre servidores de rede, switches, roteadores e storages, e 98 aplicações Web em produção.

A opção de solução selecionada, conforme indicado no item VI, foi a nº 3 – Solução comercial com gerenciamento e armazenamento na rede local do Tribunal (On premise).

Assim, o valor estimado, obtido a partir dos menores valores constantes da pesquisa de preços disponível no documento SEI nº 1441027 (obtidos da proposta de empresa Servix, que representa o fabricante Tenable), é o seguinte:

Item	Descrição	Valor (R$)
1	Gestão de Vulnerabilidades para Ativos de Rede – 500 endereços IP (x2)	325.113,76
2	Gestão de Vulnerabilidades para Aplicações Web	0,00
3	Instalação e Configuração	11.322,00
4	Repasse Tecnológico	8.342,00
5	Pacotes de 4 horas de serviço	0,00
CUSTO TOTAL ESTIMADO		**344.777,76**

Observações:

1. No caso da proposta adotada como referência, a aquisição de dois pacotes de Gestão de Vulnerabilidades para Ativos de Rede para 500 endereços IP cada um (equivalente a 1000 endereços IP), apresenta valor total inferior à soma dos pacotes para 500, 250 e 128 endereços IP (equivalente a 878 endereços IP, quantidade mais próxima aos 860 ativos de rede de propriedade do TSE);
2. Na mesma proposta, a funcionalidade de Gestão de Vulnerabilidades para Aplicações Web já é integrada ao produto de Gestão de Vulnerabilidades para Ativos de Rede, sem custo adicional, razão pela qual seu custo está indicado como zero)
3. Também nesta proposta, as horas de serviço técnico já estão contempladas no licenciamento do produto, sem custo adicional, razão pela qual o custo do Item 5 também está indicado como zero.
4. O conjunto das observações acima torna a opção pela aquisição de dois pacotes para 500 endereços IP cada um mais vantajosa do que a aquisição de pacotes para 500, 250 e 128 endereços IP, embora contemple uma quantidade total de endereços IP maior.
5. O custo total estimado indicado neste ETP (R$ 344.777,76) apresenta-se inferior aos informados nos despachos SAD 1430326 e SEGTI 1431525 (R$ 600.000,00) principalmente em função do fato indicado na observação n. 2 (a proposta de menor valor traz custo zero para dois itens). A proposta de menor valor foi adotada como estimativa como forma de garantir um preço de aquisição mais baixo, entretanto, caso a administração entenda que isso se traduz em risco de licitação deserta, ou outro risco semelhante, pode-se adotar uma estimativa que considere os custos indicados para esses dois itens nas demais propostas.

XI – Aquisição anterior no TSE:	
Processo nº:	Não houve aquisições anteriores para este objeto
Fornecedor:	

Resultado da análise:	

XII – Apresente os indicadores para avaliar a economicidade, a eficácia e a efetividade:

Sugere-se a adoção dos seguintes indicadores para a avaliação da eficácia e da efetividade da solução adquirida:

- Quantidade de vulnerabilidades identificadas
- Quantidade de vulnerabilidades mitigadas
- Quantidade de incidentes de segurança decorrentes da exploração de vulnerabilidades de ativos de TI

Quanto à economicidade, como a disciplina de Gestão de Vulnerabilidades não é implementada hoje no tribunal, não há como adotar um indicador que possa fazer uma comparação entre a situação atual e a situação futura.

XIII – Indicação orçamentária:

A disponibilidade será informada posteriormente pela Secretaria de Planejamento, Orçamento, Finanças e Contabilidade (SOF)

XIV – Observações:

Pretendemos realizar a presente contratação de forma conjunta com o TRE-PB e outros tribunais eleitorais. A realização da contratação por parte daquele tribunal foi registrada no Portal de Aquisições de TI da Justiça Eleitoral (http://sticonhecimento.tse.jus.br/informes/2020/portal-de-aquisicoes-de-ti), classificada sob o tema "Serviço de TI: Consultoria ou Serviço Especializado", e sob o objeto "Subscrição de ferramenta de gestão de vulnerabilidades". A contratação está sendo formalizada, no âmbito do TRE-PB, sob o processo SEI 0008787-53.2020.6.15.8000 daquele regional.

XV – Assinatura do servidor ou da equipe de planejamento da contratação responsável pela elaboração deste documento:

CARLOS EDUARDO MIRANDA ZOTTMANN
CHEFE DE SEÇÃO

Documento assinado eletronicamente em **23/10/2020, às 18:08**, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.

A autenticidade do documento pode ser conferida em https://sei.tse.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0&cv=1475600&crc=7C52F6F1, informando, caso não preenchido, o código verificador **1475600** e o código CRC **7C52F6F1**.

TRIBUNAL SUPERIOR ELEITORAL

ESTUDOS PRELIMINARES DA CONTRATAÇÃO

I – Apresente a necessidade a ser atendida:

Realizar a Gestão de Vulnerabilidades em Ativos de Tecnologia da Informação

II – Indique o público-alvo (unidades orgânicas, autoridades, servidores, outros) da contratação:

A Gestão de Vulnerabilidades em Ativos de Tecnologia da Informação é uma atividade a ser executada pela Secretaria de Tecnologia da Informação. Tais ativos, entretanto, suportam todas os sistemas e aplicações utilizadas pelas diversas unidades organizacionais do tribunal.

III – Indique a(s) consequência(s), caso não haja atendimento da necessidade:

Vulnerabilidades em Ativos de Tecnologia da Informação representam as fraquezas existentes nesses ativos que podem ser exploradas por atacantes para a realização de ataques cibernéticos. A Gestão de Vulnerabilidades é uma disciplina que permite a identificação, classificação em termos de severidade, e priorização no tratamento de vulnerabilidades. A não realização da Gestão de Vulnerabilidades mantém alto o nível de risco do ambiente de Tecnologia da Informação, expondo os sistemas e aplicações do tribunal a ataques, facilitando a ocorrência de incidentes de segurança tais como divulgação não autorizada de informações sensíveis, adulteração de informações, etc., o que pode causar prejuízos materiais e de imagem ao tribunal.

IV – Indique o alinhamento da necessidade ao Planejamento Estratégico do TSE:

Conforme indicado no Documento de Oficialização de Demandas, a aquisição está alinhada ao Planejamento Estratégico da seguinte forma:

Objetivo Estratégico Institucional:

OE11 – Garantir a eficiência na prestação dos serviços de tecnologia da informação e comunicação

Planejamento Estratégico de TI

OETIC 7–Aprimorar as práticas e os controles de segurança da informação utilizados no desenvolvimento e na operação de serviços e de soluções de TI

IN07.01Implementar iniciativas que visam ao aprimoramento das práticas e dos controles de segurança da informação utilizados no desenvolvimento e na operação de serviços e soluções de TIC providas pela STI.

V – Indique o resultado da pesquisa de mercado feita para identificação das diferentes soluções que possam atender às necessidades explicitadas:

	Solução identificada	Detalhamento das Soluções
1ª	Soluções disponibilizadas de forma gratuita	Ferramentas disponibilizadas sob a modalidade de software livres (código aberto) ou gratuitamente, como os softwares OpenVas e Nmap
2ª	Solução comercial com gerenciamento e armazenamento na nuvem (On Cloud)	Aquisição de software de gerenciamento de vulnerabilidades e análise dinâmica de aplicações web baseado em nuvem, com modelo de subscrição por tempo determinado

3ª	Solução comercial com gerenciamento e armazenamento na rede local do Tribunal (On premise)	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 tempo determinado, ou de licença perpetua com suporte técnico por tempo determinado

A pesquisa de preços referente às opções comerciais encontra-se no documento SEI 1441027.

Faz-se importante destacar que trata-se de solução de prateleira, com produtos similares desenvolvidos por diferentes fabricantes, usualmente disponível no mercado para contratação por órgãos públicos e entidades privadas, razão pela qual não é cabível a indicação, para cada solução, dos órgãos públicos ou entidades que as tenham adotado.

Quanto à quantidade de soluções comerciais, observamos que a quantidade de fabricantes é pequena, que, entretanto, contam com uma rede razoável de revendas no mercado nacional. As especificações técnicas procuraram refletir as necessidades técnicas do tribunal, sem a inserção de exigências injustificadas. Questões de segurança, entretanto, foram consideradas, e serão detalhadas no trecho referente à escolha da solução.

Vantagens e Desvantagens de cada solução

Opção nº 1, "Soluções disponibilizadas de forma gratuita":

Vantagens:

Essas soluções não apresentam custo de aquisição, uma vez que são disponibilizada de forma gratuita por seus fabricantes, ou ainda no formato de código aberto, onde toda a comunidade pode ter acesso ao código fonte dos diversos programas que as compõem.

Desvantagens:

Atendem apenas parte da necessidade, uma vez que tais soluções não contam com suporte técnico especializado, sua frequência de atualização da base de vulnerabilidades é inferior às alternativas comerciais, e não dispõem de funções importantes como a existência de fontes de inteligência sobre ameaças (*Threat Intelligence*) e funcionalidades avançadas de priorização da mitigação de vulnerabilidades. Outro ponto desfavorável com relação a esta opção é que os relatórios fornecidos não apresentam rastreabilidade das atividades já realizadas nos ativos e sistemas.

Obs: Faz-se importante destacar que o tribunal já se utiliza da solução OpenVAS, uma das representantes das soluções gratuitas, e a existência dessas limitações é a motivação para a realização da presente aquisição.

Opção nº 2, "Solução comercial com gerenciamento e armazenamento na nuvem (On Cloud)":

Vantagens:

Atendem todos os requisitos de funcionalidades descritas na especificação da solução, fornecendo todas as funcionalidades apontadas como desvantagens relacionadas à Opção 1.

Adicionalmente, apresenta facilidade de gerenciamento, uma vez que o componente central da solução é provido em ambiente de nuvem pública, não sendo necessário o esforço, por parte do tribunal, para instalação, configuração e eventuais atualizações do ambiente, uma vez que todas essas tarefas são de responsabilidade do próprio fabricante, em função da natureza da solução.

Desvantagens:

Como pontos negativos apontamos o fato de os dados armazenados pela ferramenta (vulnerabilidades dos ativos de TIC), que são de natureza sensível, serem armazenados em nuvem pública, e o fato de que, ao final do período de subscrição, o acesso à ferramenta é completamente indisponibilizado ao tribunal, inviabilizando até mesmo as consultas às análises de vulnerabilidades previamente conduzidas.

A opção nº 3, "Solução comercial com gerenciamento e armazenamento na rede local do Tribunal (On premise)":

Vantagens:

Todos os requisitos de funcionalidades do projeto também são atendidos por esse cenário.

Apresenta um menor risco de vazamento de dados sensíveis que são as vulnerabilidades dos ativos de TIC, pois os mesmos serão armazenados localmente e não em nuvem pública.

Outro ponto favorável é o fato de que após o término do período de suporte contratado, o tribunal continuará a ter acesso à ferramenta, embora sem o direito de recebimento de atualizações de versão e de novas vulnerabilidades. Ainda que tal acesso não seja o mais adequado para a realização de novas análises de vulnerabilidades, em razão de sua desatualização, todas as análises previamente realizadas permanecem acessíveis, facilitando a tarefa de correção dos problemas encontrados.

Desvantagens:

Traz para o tribunal o esforço de atualização da solução (por meio de mão de obra própria ou de previsão contratual para execução por parte da empresa contratada), uma vez que a mesma passa a estar instalada em nosso próprio ambiente de TI.

Outros órgãos públicos que adotaram soluções de Gestão de Vulnerabilidades

Nas pesquisas que realizamos identificamos os seguintes órgãos públicos como exemplos de entidades que já realizaram a aquisição de soluções de Gestão de Vulnerabilidades:

- Banrisul (Pregão Eletrônico nº 509/2019 - documento 1472768): Solução de Gestão de Vulnerabilidades na modalidade de instalação local
- Conselho da Justiça Federal (Pregão Eletrônico nº 1/2020 - documento 1472778): Gestão de Vulnerabilidades como parte de um conjunto de Serviços Gerenciados de Segurança da Informação
- INEP (Termo de Referência - Processo 23036.001606/2017-15 - documento 1472784): Gestão de Vulnerabilidades na modalidade de instalação local, como parte de um conjunto de Serviços Gerenciados de Segurança
- Superior Tribunal de Justiça (Contrato STJ 86/2018 - documento 1472790): Solução de Gestão de Vulnerabilidades na modalidade de instalação local
- Tribunal Regional Eleitoral do Paraná (ARP 3/2020 - documento 1472800): Solução de Gestão de Vulnerabilidades na modalidade nuvem pública.

VI – Indique a descrição completa da solução que, por entendimento do(s) signatário(s) deste documento, melhor atenderá à necessidade especificada neste documento:

Especificação Técnica da Solução

1. Deve estar licenciada de tal forma que estejam inclusas todas as funcionalidades para realizar varreduras de vulnerabilidades, avaliação de configuração e conformidade (*baseline*

e compliance), indícios e padrões de códigos maliciosos conhecidos (malware).
2. Deve ser licenciada para um número ilimitado de scanners (prevendo redundância);
3. Todas as licenças de uso de software devem ser registradas no site do fabricante, na data da entrega, em nome da Contratante;
4. Deve possuir recurso de varredura ativa, onde o scanner comunica-se com os alvos (ativos) através da rede;
5. Deve permitir mecanismo de varredura baseado em inferência com técnicas de varredura não intrusivas;
6. Deve suportar varreduras de dispositivos de *IoT* (Internet das Coisas);
7. Deve ser capaz de identificar no mínimo 50.000 *CVEs* (*Common Vulnerabilities and Exposures*);
8. 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;
9. Deve atribuir a todas as vulnerabilidades uma severidade baseada no *CVSSv3 score*;
10. Deve calcular a criticidade com base nos dados agregados e consolidados do ativo, dados de segurança, sistema e conformidade, bem como hierarquias e prioridades;
11. Deve fornecer criptografia de ponta a ponta (envolvendo coleta, transmissão e armazenamento) dos dados referentes aos ativos avaliados, vulnerabilidades identificadas, e outras informações sobre o ambiente do tribunal;
12. Deve possuir a capacidade de armazenar informações dos ativos descobertos no ambiente;
13. Deve possuir um sistema de busca de informações de um determinado ativo com no mínimo as seguintes características;
    1. Por sistema operacional;
    2. Por um determinado software instalado;
    3. Por Ativos impactados por uma determinada vulnerabilidade.
14. Deve possuir suporte para a adição de detecções personalizadas usando o *OVAL (Open Vulnerability Assessment Language)*;
15. Deve permitir aceitar o risco de uma determinada vulnerabilidade encontrada no ambiente;
16. Deve possibilitar alterar a criticidade de determinada vulnerabilidade de forma manual;
17. Deve possuir um sistema de pontuação e priorização das vulnerabilidades;
18. Deve ser capaz de aplicar algoritmos de aprendizagem de máquina *(machine learning*) para analisar as características relacionadas a vulnerabilidades;
19. O sistema de pontuação e priorização de vulnerabilidades deve avaliar no mínimo as seguintes características:
    1. *CVSSv3 Impact Score*;
    2. Idade da Vulnerabilidade;
    3. Se existe ameaça ou *exploit* publicados que explorem a vulnerabilidade;
    4. Número de produtos afetados pela vulnerabilidade;
20. Deve ser capaz de fazer a correlação em tempo real de ameaças ativas contra vulnerabilidades encontradas, incluindo *feeds* de inteligência de ameaças ao vivo;
21. Deve possuir uma API para automação de processos e integração com aplicações terceiras permitindo, no mínimo, a extração de dados para carga em soluções de *SIEM (Security Information and Event Management)*;
22. Deve possuir uma API para automação de processos e integração com aplicações ITSM *(Information Technology Service Management)* do órgão para a abertura de chamados técnicos referentes às vulnerabilidades encontradas, permitindo o agrupamento no chamado por ações corretivas;
23. Deve permitir a instalação de agentes em estações de trabalho e servidores, para varredura diretamente no sistema operacional;
24. Deve possuir conectores para, no mínimo, as seguintes plataformas de serviços em nuvem:
    1. Amazon Web Service (AWS);
    2. Microsoft Azure;
    3. Google Cloud Platform.

25. Deve possuir recurso de monitoria passiva do tráfego de rede para identificação de anomalias, novos dispositivos e desvios de padrões observados;
26. Deve ser licenciada para o uso ilimitado de sensores passivos de rede para realizar o monitoramento em tempo real;
27. Deve possuir sensores, no mínimo, com as seguintes funcionalidades:
    1. Execução de verificação completa do sistema (rede), adequada para qualquer ativo;
    2. Verificação sem recomendações da rede, para que se possa personalizar totalmente as configurações da verificação;
    3. Autenticação de ativos e enumeração de atualizações ausentes;
    4. Execução de varredura simples para descobrir ativos em operação e portas TCP/UDP abertas;
    5. Utilização de um scanner para verificar aplicativos da web;
    6. Avaliação de dispositivos móveis
    7. Auditoria de configuração de serviços em nuvem de terceiros;
    8. Auditoria de configuração dos gerenciadores de dispositivos móveis;
    9. Auditoria de configuração dos dispositivos de rede;
    10. Auditoria de configurações do sistema em relação a uma linha de base conhecida;
    11. Detecção de desvio de segurança Intel AMT;
    12. Verificação de malware nos sistemas Windows e Unix;
28. Deve ser possível determinar em tempo real quais portas de serviços (UDP/TCP) estão abertas em determinado ativo;
29. Deve ser capaz de realizar em tempo real a descoberta de novos ativos para no minímo:
    1. Bancos de dados;
    2. Hypervisors (no mímino VMWare ESX/ESXi);
    3. Dispositivos móveis;
    4. Dispositivos de rede;
    5. Endpoints;
    6. Aplicações;
30. Deve ser capaz de, em tempo real, detectar logins e downloads de arquivos em um compartilhamento de rede;
31. Permitir identificar vulnerabilidades associadas a servidores SQL no tráfego de rede;
32. Deve possuir interface para integração com as principais soluções de *SIEM (Security Information and Event Management)* de mercado, tais como IBM QRadar, Microfocus ArcSight e Splunk;
33. 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.
34. A atualização das bases de conhecimento sobre vulnerabilidades e ameaças deve ocorrer diariamente e sem interrupção dos serviços.
35. Configuração de segurança e acesso à gerência da solução:
    1. Todos os dados armazenados nos servidores da solução devem ser criptografados e possuir logs de acesso;
    2. As conexões para o envio de dados devem ser estabelecidas utilizando-se no mínimo o algoritmo TLS 1.2 de chave 2048 bits;
    3. Os dados em trânsito devem ser criptografados ao menos com o algoritmo AES-128 bits;
    4. As funções de hash devem usar ao menos o algoritmo SHA-256;
    5. Os dados armazenados devem ser criptografados ao menos com o algoritmo AES-256 bits;
    6. Será aceito como comprovação dos critérios de criptografia a publicação em site do fabricante ou declaração do próprio fabricante;
    7. Somente servidores da Contratante ou pessoa por ela autorizada poderão ter acesso aos dados da solução;

8. A solução deve permitir a criação de, no mínimo, 20 contas para gerência e acesso aos relatórios, sem custo adicional;
9. A empresa contratada não deverá ter acesso à rede interna da Contratante e, em caso de opção pela utilização da solução hospedada em nuvem, todo tráfego de dados de saída deverá ser iniciado pelos scanners instalados no ambiente de TI da própria Contratada.

36. Deve ser capaz de produzir relatórios nos seguintes formatos: PDF, CSV, HTML e no formato de texto que poderá ser DOCX ou RTF;
    1. Deve ser capaz de executar relatórios periódicos de acordo com a frequência estabelecida pelo administrador, bem como a geração de relatórios sob demanda;
    2. A solução deve possibilitar a criação de relatórios baseados na seleção de ativos, permitindo inclusive a seleção de todos os ativos existentes;
    3. Deve suportar a criação de relatórios criptografados (protegidos por senha configurável) ;
    4. Deve suportar o envio automático de relatórios para destinatários específicos;
    5. Deve ser possível definir a frequência na geração dos relatórios para no mínimo: Diário, Mensal, Semanal e Anual;
    6. Permitir especificar níveis de permissão nos relatórios para usuários e grupos específicos;
    7. Deve fornecer relatórios do tipo *"scorecard"* para as partes interessadas da empresa;
    8. Deve fornecer relatórios de correções aplicadas, classificados pelos seguintes critérios: grupo de ativos, usuários e vulnerabilidades;
37. A solução deve possuir ou permitir a criação de relatórios com as seguintes informações:
    1. Ativos verificados sem credenciais;
    2. Vulnerabilidades mais críticas;
    3. Ativos mais infectados por Malwares;
    4. Ativos exploráveis por Malwares;
    5. Total de vulnerabilidades que podem ser exploradas por meio da plataforma Metasploit;
    6. Vulnerabilidades críticas e exploráveis;
    7. Ativos com vulnerabilidades que podem ser exploradas;
38. A solução deve possuir dashboards customizáveis onde o administrador pode criar, editar ou remover painéis de acordo com a necessidade;
39. A solução deve ser capaz de realizar o inventário básico de todos os ativos da rede local e publicados na Internet, sem limites de endereços IP, coletando ao menos as informações sobre nome do ativo, endereço IP e Sistema Operacional.
40. Deve permitir a configuração de vários painéis e widgets;
41. Deve ser capaz de medir e reportar ameaças;
42. Deve ser capaz de visualizar ameaças críticas ao ambiente monitorado;
43. 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
44. A plataforma de software deve suportar vários mecanismos de varredura distribuídos em diferentes localidades e regiões e gerenciar todos por uma console central;
45. 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;
46. A plataforma de software deve permitir o monitoramento através de agentes instalados, até o limite de licenças adquiridas, para varredura diretamente no sistema operacional.
47. 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.
48. 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;
49. 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;
50. A plataforma de software deve ser configurável para permitir a otimização das parametrizações de varredura;
51. 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;
52. A plataforma de software deve fornecer a capacidade de escalar privilégios nos destinos, do acesso de usuário padrão até acesso de sistema ou administrativo;
53. A plataforma de software deve ser capaz de realizar pesquisas de dados confidenciais.
54. 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;
55. 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;
56. A solução de análise deve ser capaz de analisar, testar e reportar falhas de segurança em aplicações Web;
57. A solução de análise deverá ser capaz de executar varreduras em sistemas Web através de seus endereços IP ou FQDN (DNS);
58. A solução de análise deve ser capaz de identificar vulnerabilidades de divulgação de dados, como vazamento de informações de identificação pessoal;
59. Para varreduras do tipo extensas e detalhadas, deve varrer e auditar no mínimo os seguintes elementos:
    1. *Cookies, Headers*, Formulários e *Links*;
    2. Nomes e valores de parâmetros da aplicação;
    3. Elementos *JSON* e *XML*;
    4. Elementos *DOM*;
60. Deverá também permitir a execução da função *crawler*, que consiste na navegação para descoberta das *URLs* existentes na aplicação;
61. A solução de análise deve suportar a integração com os softwares de automação de testes para permitir sequências de autenticação complexas;
62. A solução de análise deve ser capaz de realizar testes/varreduras em aplicações separadas, simultaneamente limitadas ao número de licenças;
63. Suporte a ferramentas para construção de requisições e análise de respostas de aplicações *WEB*, *API's* e *WebServices*, tais como *Postman Collections*;
64. A solução de análise deve oferecer suporte à capacidade de testar novamente a vulnerabilidade específica que foi detectada anteriormente no aplicativo *Web*;
65. Deve ser capaz de utilizar scripts customizados de *crawling* com parâmetros definidos pelo usuário;
66. Deve ser capaz de excluir determinadas *URLs* da varredura através de expressões regulares;
67. Deve ser capaz de excluir determinados tipos de arquivos através de suas extensões;
68. Deve ser capaz de instituir no mínimo os seguintes limites:
    1. Número máximo de *URLs* para *crawling* e navegação;
    2. Número máximo de diretórios para varreduras;
    3. Número máximo de elementos *DOM*;
    4. Tamanho máximo de respostas;
    5. Tempo máximo para a varredura;
    6. Número máximo de conexões HTTP(S) ao servidor hospedando a aplicação *Web*;
    7. Número máximo de requisições HTTP(S) por segundo;
69. Deve ser capaz de agendar a varredura e determinar sua frequência entre uma única vez, diária, semanal, mensal e anual;
70. Deve suportar o envio de notificações por email;

71. Deverá ser compatível com avaliação de *web services REST e SOAP*;
72. A solução de análise deve suportar os seguintes esquemas de autenticação:
    1. Autenticação Básica (*Digest*);
    2. *NTLM*;
    3. Autenticação de *Cookies*;
73. Deve ser capaz de importar scripts de autenticação previamente configurados pelo usuário;
74. 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;
75. Os resultados devem ser apresentados agregados por vulnerabilidades ou por aplicações;
76. Para cada vulnerabilidade encontrada, devem ser exibidos detalhes e evidências;
77. Cada vulnerabilidade encontrada deve conter também soluções propostas para mitigação ou remediação;
78. Serviço de Detecção de Malware:
    1. Deve utilizar a plataforma de gerenciamento de vulnerabilidades existente;
    2. Deve permitir visualizar o acompanhamento das atividades de verificação, páginas infectadas e tendências de infecção por malware;
    3. 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.
79. A solução deve ser capaz de realizar varreduras nos seguintes componentes/aplicações:
    1. WordPress;
    2. IIS 6.x e IIS 10.x;
    3. ASP 6;
    4. .NET 2;
    5. Apache HTTPD 2.2.x e 2.4.x;
    6. Tomcat 6.x, 7.x, 8.x e superiores;
    7. Jetty 8 e superiores;
    8. Nginx;
    9. PHP 5.3.x, 5.4.x, 5.6.x, 7.0.x e 7.1.x e superiores;
    10. Java 1.5, 1.6, 1.7 e 1.8 e superiores;
    11. Jboss 4.x e 7.x e superiores;
    12. WildFly 8 e 10 e superiores;
    13. Plone 2.5.x e 5.2.1.41.x e superiores;
    14. Zope;
    15. Python 2.4.4 e superiores;
    16. J2EE;
    17. Ansible;
    18. Joomla;
    19. Moodle;
    20. Docker Conteiner;
    21. ELK;
    22. GIT;
    23. Grafana; e
    24. Redmine.

Obs: A especificação técnica prevê compatibilidade com plataformas de nuvem pública (Amazon AWS, Microsoft Azure e Google Cloud) e com alguns produtos disponibilizados sob a modalidade de software livre (Joomla e Wordpress) que, embora não sejam atualmente utilizados pelo TSE, são produtos padrão de mercado, que podem vir a ser utilizados pelo tribunal em virtude de novos projetos. Tal previsão de compatibilidade tem o condão de evitar a aquisição de um produto de Gestão de Vulnerabilidades que facilmente se torne incompatível com o parque de Tecnologia da Informação do tribunal.

Serviços de Instalação e Configuração

A Contratada deverá instalar a solução e configurá-la para a utilização por parte do Tribunal Superior Eleitoral.

Deverá ainda realizar as atualizações da solução, conforme liberação de novas versões por parte do fabricante.

Requisitos de Capacitação

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

Requisitos Temporais

Prazos

A Contratada terá 15 (quinze) dias corridos, contados da assinatura do contrato, para fornecer os softwares ou as subscrições contratadas;

A Contratada terá 15 (quinze) dias corridos, contados a partir do fornecimento, para realizar a instalação e configuração da solução.

Suporte e garantia

O Suporte remoto por parte do fabricante, bem como a garantia de atualização do software devem ser de, no mínimo, 36 (trinta e seis) meses.

Requisitos de Segurança

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 Superior Eleitoral aos quais tiver acesso em decorrência do objeto da presente contratação, ficando terminantemente proibida de fazer uso ou revelação destes sob qualquer justificativa;

O Tribunal Superior Eleitoral terá propriedade sobre todos os documentos e procedimentos operacionais produzidos no escopo da presente contratação;

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

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.

Requisitos Sociais, Ambientais e culturais

- A solução deve ser disponibilizada para instalação, e seus manuais devem ser disponibilizados para acesso, de forma *on-line*, sem o uso de dispositivos físicos;
- A contratada não deve possuir inscrição no cadastro de empregadores flagrados explorando trabalhadores em condições análogas às de escravo;
- A contratada, ou seus dirigentes, não deve ter sido condenada por infringir as leis de combate à discriminação de raça ou de gênero, ao trabalho infantil e ao trabalho escravo;
- Apresentação do Programa de Controle Médico de Saúde Ocupacional (PCMSO);

- Apresentação do Programa de Prevenção de Riscos Ambientais (PPRA);
- Atendimento ao art. 93 da Lei nº 8.213/91

Transição Contratual

Não é necessária a previsão de atividades de transição contratual. Não há contrato anterior para o mesmo objeto, e o objeto é o fornecimento de uma solução para utilização por parte do tribunal sem a execução de serviços associados por parte da Contratada, à exceção da instalação e configuração da solução, e do suporte remoto por parte do fabricante para a resolução de eventuais problemas apresentados pelo produto e para o esclarecimento de dúvidas de utilização.

Benefícios Diretos e Indiretos pretendidos com a contratação

Conforme informado no Documento de Oficialização de Demanda, os Resultados a Serem Alcançados, que trazem em si os benefícios pretendidos com a contratação, são os seguintes:

- Identificação das vulnerabilidades das soluções de TIC utilizadas pelo TSE.

- Redução do nível de risco do ambiente de TIC por meio da correção das vulnerabilidades identificadas;

Necessidade de serviços de manutenção

A necessidade de serviços de manutenção já se encontra prevista no item "Serviços de Instalação e Configuração", que prevê a necessidade de atualizações do produto por ocasião da liberação de versões por parte do fabricante, e na exigência de suporte técnico remoto pelo fabricante.

Formação e experiência profissional da equipe que realizará os serviços

A equipe que realizará os serviços de instalação, configuração e atualização de versões deverá possuir certificação emitida pelo fabricante, em modalidade que ateste que a equipe está qualificada para a realização de tais serviços.

Seleção da solução

A opção nº 1 representa o tipo de solução que já se encontra em utilização no tribunal atualmente, e, como suas limitações são o motivo que enseja a contratação ora almejada, é uma opção naturalmente descartada.

Com relação ao nível de segurança associado às opções nº 2 e nº 3, em razão da diferença entre a hospedagem da solução em nuvem pública ou no próprio ambiente de TI do tribunal, gostaríamos de destacar as recomendações constantes da Norma Complementar nº 14/IN01 do Departamento de Segurança da Informação e Comunicações (DSIC), subordinado ao Gabinete de Segurança Institucional da Presidência da República, que diz o seguinte:

> *"5.2.2 Informação sigilosa: como regra geral, deve ser evitado o tratamento em ambiente de computação em nuvem, conforme disposições a seguir:*
>
> *5.2.2.1. Informação classificada: é vedado o tratamento em ambiente de computação em nuvem;*
>
> *5.2.2.2. Conhecimento e informação contida em material de acesso restrito: é vedado o tratamento em ambiente de computação em nuvem;*
>
> ....
>
> *5.3 Deve ser assegurado que dados, metadados, informações e conhecimento, produzidos ou custodiados por órgão ou entidade da APF, bem como suas cópias de segurança, residam em território brasileiro;"*

Observa-se que existe a vedação do armazenamento de informação classificada ou de acesso restrito em ambientes de nuvem, além da recomendação de que os dados produzidos ou custodiados por órgão ou entidade da APF residam em território brasileiro.

Muito embora as informações referentes às vulnerabilidades de ativos de TI não tenham sido formalmente classificadas como sigilosas ou de acesso restrito, podemos afirmar que são informações que devem ser de conhecimento de um grupo restrito de profissionais, responsáveis pelo tratamento de risco e pelas configurações de segurança do ambiente de TI do tribunal. Adotando-se tais vedações como boa prática de segurança no tratamento de informações sobre vulnerabilidades conhecidas em ativos de TI do tribunal, temos que seria ao menos recomendado seu armazenamento em ambiente interno.

Adicionalmente, as soluções hospedadas em nuvem, de acordo com a pesquisa de mercado realizada, ainda não oferecem a opção de hospedagem em ambiente de nuvem localizado em território brasileiro.

Destacamos ainda que a pesquisa de preços disponibilizada no documento 1441027 evidencia que não há grande disparidade entre os preços de ambos os tipos de solução.

Sendo assim, a alternativa selecionada é a opção nº 3, "Solução comercial com gerenciamento e armazenamento na rede local do Tribunal (On premise)", tendo em vista seu o menor preço e sua maior segurança quanto à confidencialidade das informações sobre os ativos de TI e suas vulnerabilidades.

Com relação ao prazo de licenciamento, indicamos o prazo de 36 meses, ainda que seu custo relativo, calculado por mês, seja superior ao custo do prazo de 60 meses. Tal opção se dá em função da dinamicidade das mudanças que ocorrem no cenário de tecnologia da informação, de forma tal que, após 36 meses de utilização do produto, seja recomendável uma nova avaliação de mercado para determinar as especificações técnicas mas adequadas às necessidades do tribunal.

VII – Indique o(s) estudo(s) realizado(s) ou o(s) critério(s) adotado(s) para definir o cálculo e a quantidade da necessidade:

O licenciamento das soluções de gestão de vulnerabilidades está diretamente relacionado à quantidade de endereços IP serão monitorados. Como regra geral podemos afirmar que cada Ativo de Tecnologia da Informação possui um endereço IP a ele associado. Há algumas exceções, em que um determinado ativo pode ter mais de um endereço IP utilizado para finalidades distintas, porém é uma situação que ocorre em poucos ativos que, mesmo assim, podem ter suas vulnerabilidades gerenciadas a partir de um único endereço IP.

Já para a análise dinâmica de vulnerabilidades de aplicações WEB, as soluções apresentadas estão vinculadas aos endereços Web das aplicações (endereço digitado no navegador web para acesso a uma determinada aplicação), independentemente do quantitativo de instâncias ou servidores em que essas aplicações estejam sendo executadas. Para a estimativa de aplicações a serem monitoradas, contabilizamos apenas as aplicações disponibilizadas na Internet, por serem as mais vulneráveis a ataques.

A partir das observações acima, elaboramos os seguintes quadros, detalhando as quantidades de ativos de TI e de Aplicações executadas no ambiente do TSE

Quadro 1 – Ativos de TI

Tipo de ativo	**Quantidade**
Máquinas virtuais (VM)	800
Roteadores	8
Switch de rede primário (núcleo da rede)	3
Switch de rede secundário (camada de distribuição)	12
Switch de rede terciário (camada de acesso)	31
Balanceador de links de internet	4
Storages (equipamentos para armazenamento de dados)	2
TOTAL	**860**

Obs: Informações extraídas das consoles de gerenciamentos dos ambientes de TI do tribunal.

Quadro 2 – Aplicações disponibilizadas na Internet

Aplicação	**Ambiente**
api-migra-ccontrato-dev.tse.jus.b	Desenvolvimento
apps-desenvolvimento.tse.jus.br	Desenvolvimento
justifica-dsv.tse.jus.br	Desenvolvimento
api-services-hmg.tse.jus.br	Homologação
autentica-hmg.tse.jus.br	Homologação
candex-api-simulado.tse.jus.br	Homologação
jet-homologacao.tse.jus.br	Homologação
login-hmg.tse.jus.br	Homologação
pjehmg.tse.jus.br	Homologação
pjezona-hmg.tse.jus.br	Homologação
acoeseducacionais.tse.jus.br	Produção
agencia.tse.jus.br	Produção
agenciaje.tse.jus.br	Produção
akira.tse.jus.br	Produção
api.tse.jus.br	Produção
api-justifica.tse.jus.br	Produção
api-migra-ccontrato.tse.jus.br	Produção

api-services.tse.jus.br	Produção
apps.tse.jus.br	Produção
appsinfovia01.tse.jus.br	Produção
appsinter.tse.jus.br	Produção
appspjetse03.tse.jus.br	Produção
arquivos.tse.jus.br	Produção
autentica.tse.jus.br	Produção
biblioteca.tse.jus.br	Produção
bibliotecadigital.tse.jus.br	Produção
bioex.tse.jus.br	Produção
candex-api-oficial.tse.jus.br	Produção
candex-atualizador.tse.jus.br	Produção
cdn.tse.jus.br	Produção
chimera.tse.jus.br	Produção
consultapublicapje.tse.jus.br	Produção
coyote.tse.jus.br	Produção
coyote-api.tse.jus.br	Produção
credenciamento.tse.jus.br	Produção
democraciatododia.tse.jus.br	Produção

dft.tse.jus.br	Produção
divulga.tse.jus.br	Produção
divulgacandcontas.tse.jus.br	Produção
divulgacao-resultados.tse.jus.br	Produção
divulgaspca.tse.jus.br	Produção
dje-consulta.tse.jus.br	Produção
dni.tse.jus.br	Produção
download.tse.jus.br	Produção
eadeje.tse.jus.br	Produção
educacao.tse.jus.br	Produção
english.tse.jus.br	Produção
filia-consulta.tse.jus.br	Produção
filia-externo.tse.jus.br	Produção
filiaweb.tse.jus.br	Produção
financiamentocoletivo.tse.jus.br	Produção
fiscalizaje.tse.jus.br	Produção
gel.tse.jus.br	Produção
gsti.tse.jus.br	Produção
horus.tse.jus.br	Produção

idc.tse.jus.br	Produção
inter01.tse.jus.br	Produção
inter02.tse.jus.br	Produção
inter03.tse.jus.br	Produção
inter04.tse.jus.br	Produção
investigador-tps.tse.jus.br	Produção
jet.tse.jus.br	Produção
justifica.tse.jus.br	Produção
luna.tse.jus.br	Produção
mimic.tse.jus.br	Produção
miss.tse.jus.br	Produção
molly.tse.jus.br	Produção
mural-consulta.tse.jus.br	Produção
niagara.tse.jus.br	Produção
nova.tse.jus.br	Produção
orion.tse.jus.br	Produção
pardal.tse.jus.br	Produção
pesqele.tse.jus.br	Produção
phoenix.tse.jus.br	Produção

pje.tse.jus.br	Produção
pje1g.tse.jus.br	Produção
pje1g-ead.tse.jus.br	Produção
pje2advo.tse.jus.br	Produção
pje2-advo.tse.jus.br	Produção
pje3g-ead.tse.jus.br	Produção
pjefrontend.tse.jus.br	Produção
pjefrontend-ead.tse.jus.br	Produção
qrcodenobu.tse.jus.br	Produção
reje.tse.jus.br	Produção
sacexterno.tse.jus.br	Produção
schemas.tse.jus.br	Produção
sedesc1-jud-01.tse.jus.br	Produção
seer.tse.jus.br	Produção
servicedesk.tse.jus.br	Produção
servicos.tse.jus.br	Produção
servicosdeti.tse.jus.br	Produção
sessao.tse.jus.br	Produção
sge.tse.jus.br	Produção

sherlock.tse.jus.br	Produção
sico-consulta-web.tse.jus.br	Produção
simba.tse.jus.br	Produção
sintse.tse.jus.br	Produção
sle.tse.jus.br	Produção
spcadownload.tse.jus.br	Produção
spce2010.tse.jus.br	Produção
spcedownload.tse.jus.br	Produção
spceenvio.tse.jus.br	Produção
sulu.tse.jus.br	Produção
temasselecionados.tse.jus.br	Produção
testlink-fabrica.tse.jus.br	Produção
vpn.tse.jus.br	Produção
www.tse.jus.br	Produção
zodiac4.tse.jus.br	Produção
TOTAIS	
Aplicações em Produção	98
Aplicações em Homologação	7
Aplicações em Desenvolvimento	3

Obs: Informações extraídas do ambiente de gerenciamento de aplicações disponibilizadas para a Internet do tribunal. A aquisição pretendida terá como alvo apenas as aplicações disponibilizadas para a Internet em ambiente de produção, equivalente, portanto, a 98 aplicações. É importante observar que este número de aplicações pode variar ao longo do tempo, a depender do desenvolvimento e publicação de novas aplicações, ou do encerramento do ciclo de vida de aplicações ora em produção.

VIII – Indique se a solução eleita é divisível ou não, levando em consideração o mercado que a fornece:

A solução não é divisível, uma vez que é composta por elementos interdependentes, administrados coletivamente por uma única console central de gerenciamento.

IX – Indique, entre outras, as restrições internas de caráter técnico, operacional, regulamentar, financeiro e orçamentário, que possam dificultar a implementação da solução eleita:

A principal restrição que se pode apontar para a implementação da solução eleita é a disponibilidade de pessoal para a sua correta utilização.

Entretanto, tal restrição tende a ser minimizada por meio da definição de normas e procedimentos que disciplinem a realização de Gestão de Vulnerabilidades, atividade esta que já está sendo realizada por meio do projeto "CIS Controls – Fase 1" (Processo SEI n. 2019.00.000011504-4), que, dentre seus produtos, já apresentou minuta de norma de Gestão de Vulnerabilidades, devidamente aprovada pela Comissão Técnica de Tecnologia da Informação (CTTI) e encaminhada à Comissão de Segurança da Informação (CSI) para a mesma finalidade.

X – Indique o valor estimado para a contratação:

De acordo com o Item VII deste ETP, o TSE dispõe de 860 ativos de rede, entre servidores de rede, switches, roteadores e storages, e 98 aplicações Web em produção.

A opção de solução selecionada, conforme indicado no item VI, foi a nº 3 – Solução comercial com gerenciamento e armazenamento na rede local do Tribunal (On premise).

Assim, o valor estimado, obtido a partir dos menores valores constantes da pesquisa de preços disponível no documento SEI nº 1441027 (obtidos da proposta de empresa Servix, que representa o fabricante Tenable), é o seguinte:

Item	Descrição	Valor (R$)
1	Gestão de Vulnerabilidades para Ativos de Rede – 500 endereços IP (x2)	325.113,76
2	Gestão de Vulnerabilidades para Aplicações Web	0,00
3	Instalação e Configuração	11.322,00
4	Repasse Tecnológico	8.342,00
5	Pacotes de 4 horas de serviço	0,00
CUSTO TOTAL ESTIMADO		**344.777,76**

Observações:

1. No caso da proposta adotada como referência, a aquisição de dois pacotes de Gestão de Vulnerabilidades para Ativos de Rede para 500 endereços IP cada um (equivalente a 1000 endereços IP), apresenta valor total inferior à soma dos pacotes para 500, 250 e 128 endereços IP (equivalente a 878 endereços IP, quantidade mais próxima aos 860 ativos de rede de propriedade do TSE);
2. Na mesma proposta, a funcionalidade de Gestão de Vulnerabilidades para Aplicações Web já é integrada ao produto de Gestão de Vulnerabilidades para Ativos de Rede, sem custo adicional, razão pela qual seu custo está indicado como zero)
3. Também nesta proposta, as horas de serviço técnico já estão contempladas no licenciamento do produto, sem custo adicional, razão pela qual o custo do Item 5 também está indicado como zero.
4. O conjunto das observações acima torna a opção pela aquisição de dois pacotes para 500 endereços IP cada um mais vantajosa do que a aquisição de pacotes para 500, 250 e 128 endereços IP, embora contemple uma quantidade total de endereços IP maior.
5. O custo total estimado indicado neste ETP (R$ 344.777,76) apresenta-se inferior aos informados nos despachos SAD 1430326 e SEGTI 1431525 (R$ 600.000,00) principalmente em função do fato indicado na observação n. 2 (a proposta de menor valor traz custo zero para dois itens). A proposta de menor valor foi adotada como estimativa como forma de garantir um preço de aquisição mais baixo, entretanto, caso a administração entenda que isso se traduz em risco de licitação deserta, ou outro risco semelhante, pode-se adotar uma estimativa que considere os custos indicados para esses dois itens nas demais propostas.

XI – Aquisição anterior no TSE:	
Processo nº:	Não houve aquisições anteriores para este objeto
Fornecedor:	

Resultado da análise:	

XII – Apresente os indicadores para avaliar a economicidade, a eficácia e a efetividade:

Sugere-se a adoção dos seguintes indicadores para a avaliação da eficácia e da efetividade da solução adquirida:

- Quantidade de vulnerabilidades identificadas
- Quantidade de vulnerabilidades mitigadas
- Quantidade de incidentes de segurança decorrentes da exploração de vulnerabilidades de ativos de TI

Quanto à economicidade, como a disciplina de Gestão de Vulnerabilidades não é implementada hoje no tribunal, não há como adotar um indicador que possa fazer uma comparação entre a situação atual e a situação futura.

XIII – Indicação orçamentária:

A disponibilidade será informada posteriormente pela Secretaria de Planejamento, Orçamento, Finanças e Contabilidade (SOF)

XIV – Observações:

Pretendemos realizar a presente contratação de forma conjunta com o TRE-PB e outros tribunais eleitorais. A realização da contratação por parte daquele tribunal foi registrada no Portal de Aquisições de TI da Justiça Eleitoral (http://sticonhecimento.tse.jus.br/informes/2020/portal-de-aquisicoes-de-ti), classificada sob o tema "Serviço de TI: Consultoria ou Serviço Especializado", e sob o objeto "Subscrição de ferramenta de gestão de vulnerabilidades". A contratação está sendo formalizada, no âmbito do TRE-PB, sob o processo SEI 0008787-53.2020.6.15.8000 daquele regional.

XV – Assinatura do servidor ou da equipe de planejamento da contratação responsável pela elaboração deste documento:

CARLOS EDUARDO MIRANDA ZOTTMANN
CHEFE DE SEÇÃO

Documento assinado eletronicamente em **23/10/2020, às 18:08**, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.

A autenticidade do documento pode ser conferida em https://sei.tse.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0&cv=1475600&crc=7C52F6F1, informando, caso não preenchido, o código verificador **1475600** e o código CRC **7C52F6F1**.

TRIBUNAL SUPERIOR ELEITORAL

DESPACHO

SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

APROVO os Estudos Preliminares de que trata o Parecer Técnico (SEI 1475825), emitido pela Comissão Técnica de Tecnologia da Informação - CTTI.

Encaminhe-se à Secretaria de Administração - SAD para prosseguimento.

GIUSEPPE DUTRA JANINO
SECRETÁRIO(A) DE TECNOLOGIA DA INFORMAÇÃO

Documento assinado eletronicamente em **23/10/2020, às 19:27**, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.

A autenticidade do documento pode ser conferida em https://sei.tse.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0&cv=1475895&crc=59F8C9AA, informando, caso não preenchido, o código verificador **1475895** e o código CRC **59F8C9AA**.

TRIBUNAL REGIONAL ELEITORAL DA PARAÍBA

TERMO de Referência ou Projeto Básico nº 37 / 2020 - TRE-PB/PTRE/DG/STIC/NSI

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 nosso tribunal e de outros tribunais eleitorais participes 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 DOS LOTES

Lote 01 - Solução com armazenamento e gerenciamento em Nuvem (On Cloud)				
ITEM	**QTD REGISTRADA**	**PEDIDO INICIAL***	**CATMAT / CATSER**	**DESCRIÇÃO**
1	1	0	24333	Licenciamento de plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando no mínimo 128 endereços IP, por 36 meses de uso e suporte pelo fabricante.
2	1	0	24333	Licenciamento de plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos

				de rede, contemplando no mínimo 128 endereços IP, por 60 meses de uso e suporte pelo fabricante.
3	1	0	24333	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 pelo fabricante.
4	1	0	24333	Licenciamento de plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando no mínimo 250 endereços IP, por 60 meses de uso e suporte pelo fabricante.
5	1	0	24333	Licenciamento de plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando no mínimo 500 endereços IP, por 36 meses de uso e suporte pelo fabricante.
6	1	0	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.
7	1	0	24333	Licenciamento para solução de análise dinâmica em aplicações Web, pacote para no mínimo 5 domínios (FQDN), por 36 meses de uso e suporte pelo fabricante.
8	1	0	24333	Licenciamento para solução de análise dinâmica em aplicações Web, pacote para no mínimo 5 domínios (FQDN), por 60 meses de uso e suporte pelo fabricante.
9	1	0	24333	Licenciamento para solução de análise dinâmica em aplicações Web, pacote para no mínimo 10 domínios (FQDN), por 36 meses de uso e suporte pelo fabricante.
10	1	0	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.
11	1	0	26972	Instalação e configuração da solução.
12	1	0	26972	Repasse tecnológico, com período mínimo de 20 horas.
13	50	0	26972	Bloco de 4 horas de Serviço Especializado.

Lote 02 - Solução com armazenamento e gerenciamento local (On Premise)				
14	1	0	24333	Licenciamento de plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando no mínimo 128 endereços IP, por 36 meses de uso e suporte pelo fabricante.
15	1	0	24333	Licenciamento de plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando no mínimo 128 endereços IP, por 60 meses de uso e suporte pelo fabricante.
16	1	1	24333	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 pelo fabricante.
17	1	0	24333	Licenciamento de plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando no mínimo 250 endereços IP, por 60 meses de uso e suporte pelo fabricante.
18	1	0	24333	Licenciamento de plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando no mínimo 500 endereços IP, por 36 meses de uso e suporte pelo fabricante.
19	1	0	2433	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.
20	1	1	24333	Licenciamento para solução de análise dinâmica em aplicações Web, pacote para no mínimo 5 domínios (FQDN), por 36 meses de uso e suporte pelo fabricante.
21	1	0	24333	Licenciamento para solução de análise dinâmica em aplicações Web, pacote para no mínimo 5 domínios (FQDN), por 60 meses de uso e suporte pelo fabricante.
22	1	0	24333	Licenciamento para solução de análise dinâmica em aplicações Web, pacote para no mínimo 10 domínios (FQDN), por 36 meses de uso e suporte pelo fabricante.
23	1	0	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.
24	1	1	26972	Instalação e configuração da solução.
25	1	1	26972	Repasse tecnológico, com período mínimo de 20 horas.
26	50	0	26972	4 Horas de Serviço Especializado.

***OBS:** A coluna constante no campo "**pedido inicial**" leva em conta uma previsão de pedido (que não gera obrigação), levando em conta o orçamento disponível para o ano de 2020, de forma que caso o presente processo não venha a ter sua consecução no presente exercício os quantitativos iniciais previstos na tabela ficam prejudicados.

Especificações técnicas comuns do lote 01 e lote 02:

4.1 REQUISITOS GERAIS DA SOLUÇÃO DO LOTE 01 (BASEADA EM NUVEM) E DA SOLUÇÃO DO LOTE 02 (COM GERENCIAMENTO E ARMAZENAMENTO LOCAL)

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 COMUNS DA PLATAFORMA DE SOFTWARE PARA GESTÃO DE VULNERABILIDADES DOS ITENS 01,02,03,04,05 e 06 DO LOTE 01 E DOS

ITENS 14,15,16,17,18 e 19 DO LOTE 02

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 COMUNS DO MÓDULO DE ANÁLISE DINÂMICA EM APLICAÇÕES WEB ITENS 07,08,09 e 10 DO LOTE 01 E ITENS 20,21,22,23 DO LOTE 02

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 ITEM 11 DO LOTE 01 E ITEM 24 DO LOTE 02

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 ITEM 12 DO LOTE 01 E ITEM 25 DO LOTE 02

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 (itens 12 do lote 01 e item 25 do lote 02).

4.6 Bloco de 04 Horas de Serviço Especializado ITEM 13 DO LOTE 01 E ITEM 26 DO LOTE 02

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.

4.6.3 O licitante poderá apresentar R$ 0,00 (zero reais) como o preço dos itens relacionados ao Bloco de 04 Horas de Serviço Especializado (itens 13 do lote 01 e item 26 do lote 02) caso os serviços elencados estejam incluídos no preço da solução ofertada da ferramenta de gestão de vulnerabilidades;

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 (itens 13 do lote 01 e item 26 do lote 02).

Especificações técnicas especificas do lote 01:

4.7 REQUISITOS ESPECÍFICOS DA SOLUÇÃO DO LOTE 01 BASEADA EM NUVEM

Características técnicas mínimas:

4.7.1. A solução do lote 01 deve ser baseada em nuvem pública, com scanners próprios localizados em nuvem pública e scanners instalados na infraestrutura do cliente (on-premises).
4.7.2. A solução deve possuir índice de disponibilidade mensal e anual maior ou igual a 99%;

4.7.3. A solução proposta no lote 01 deve ser de mesmo fabricante, sem adaptações ou alterações não efetuadas pelo fabricante, disponível para gerenciamento em console central web unificado, sendo toda infraestrutura de aplicações, bancos de dados de vulnerabilidades, dashboards, agentes e plugins também mantidas pelo mesmo fabricante, oferecida como serviço padrão.

4.7.4. Configuração de segurança e acesso à gerência da solução:
a) A solução deve suportar autenticação de dois fatores para os usuários;

b) A solução deve possuir proteção contra ataques de força bruta bloqueando as contas após um número determinado de tentativas de login malsucedidas;

c) Os dados da CONTRATANTE devem ser marcados com um identificador que corresponde a assinatura específica da CONTRATANTE de forma a garantir que o acesso aos dados da CONTRATANTE seja limitado a apenas a CONTRATANTE.

4.7.5. A solução deve possuir conectores para, no mínimo, as seguintes plataformas:
a) Amazon Web Service (AWS);
b) Microsoft Azure;
c) Google Clound Platform.

4.7.6. A fabricante deve possuir no mínmo as seguintes certificações de privacidade e segurança:

4.7.6.1 EU-U.S. Privacy Shield Framework;

4.7.6.2 Swiss-U.S. Privacy Shield Framework.

4.7.7. A aquisição dos itens poderá ser composta em relação ao tempo e a quantidade de ativos e aplicações Web:

4.7.7.1 Para uma solução, por 3 anos, deverão ser adquiridos uma combinação dos itens 01,03,05,07 e 09 do lote 01. Por exemplo, para atender 250 ativos e 15 aplicações web (FQDNs simultâneos), por 3 anos, serão adquiridos os itens 03, 07 e 09 do lote 01.

4.7.7.2 Para uma solução, por 5 anos, deverão ser adquiridos uma combinação dos itens 02,04,06,08 e 10 do lote 01. Por exemplo, para atender 378 ativos e 10 aplicações web (FQDNs simultâneos), por 5 anos, serão adquiridos os itens 02,04 e 10 do lote 01.

Especificações técnicas especificas do lote 02:

4.7 REQUISITOS ESPECÍFICOS DA SOLUÇÃO DO LOTE 02 COM GERENCIAMENTO E ARMAZENAMENTO NA REDE LOCAL

Características técnicas mínimas:

4.7.1. Os Solução do lote 02 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 (itens 14 ou 15 ou 16 ou 17 ou 18 ou 19 do lote 02) é pré-requisito para a contratação do módulo de análise dinâmica de aplicações web (itens 20 ou 21 ou 22 ou 23 do lote 02).

4.7.2.1 Caso a licença da plataforma de software de gestão de vulnerabilidades (itens 14 ou 15 ou 16 ou 17 ou 18 ou 19 do lote 02) contemple a análise dinâmica de aplicações web o licitante deverá apresentar R$ 0,00 (zero reais) como o preço dos itens relacionados a análise dinâmica de aplicações web (itens 20, 21, 22, 23 do lote 02).

4.7.3. A solução proposta no lote 02 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;
4.7.5. A aquisição dos itens poderá ser composta em relação ao tempo e a quantidade de ativos e aplicações Web:

4.7.5.1 Para uma solução, por 3 anos, deverão ser adquiridos uma combinação dos itens 14,16,18,20 e 22 do lote 02. Por exemplo, para atender 250 ativos e 15 aplicações web (FQDNs simultâneos), por 3 anos, serão adquiridos os itens 16, 20 e 22 do lote 02.

4.7.5.2 Para uma solução, por 5 anos, deverão ser adquiridos uma combinação dos itens 15,17,19,21 e 23 do lote 02. Por exemplo, para atender 378 ativos e 10 aplicações web (FQDNs simultâneos), por 5 anos, serão adquiridos os itens 15,17 e 23.

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. Princesa Isabel, 201 - Centro - João Pessoa
CEP: 58020-528 - Paraíba – Brasil
Telefone: (83) 3512-1200 / Fax: (83) 3512-1448

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 dos lotes 1 e 2 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 registrado no item 11 do lote 1 e no item 24 do lote 2;
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 (36 meses ou 60 meses, a depender da garantia explicitada para o item em questão), 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. Para os itens 01,02,03,04,05,06,07,08,09 e 10 do lote 1 e 14,15,16,17,18,19,20,21,22 e 23 do lote 2: o fornecimento das licenças de software deverá ocorrer em até 05 (cinco) dias úteis após a assinatura do contrato.

5.5.2. Para os itens 11 do lote 1 e 24 do lote 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. Para os itens 12 do lote 1 e 25 do lote 2 - 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. Os itens 13 do lote 1 e 26 do lote 2 - 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-PB, 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-PB 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. Para a amostra, a empresa deverá apresentar as mesmas verões do produto ofertado no certame, com técnico certificado na solução para configuração e comprovação dos itens pendentes, nas dependências deste órgão, conforme itens 1.1.1 e 1.1.2, TC-006.806/2006-4, Acórdão nº 838/2006-TCU-2ª Câmara.

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 36 meses ou 60 meses, conforme o suporte do item contratado seja de 36 ou 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-PB, 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 lotes, 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.

FELIPE CAVALCANTI ALVES
RESPONSÁVEL PELO NÚCLEO DE SEGURANÇA DA INFORMAÇÃO

Documento assinado eletronicamente por FELIPE CAVALCANTI ALVES em 22/10/2020, às 13:24, conforme art. 1º, III, "b", da Lei 11.419/2006.

JAILTON CALDEIRA BRANT
CHEFE DA SEÇÃO DE CONTRATOS

Documento assinado eletronicamente por JAILTON CALDEIRA BRANT em 22/10/2020, às 13:35, conforme art. 1º, III, "b", da Lei 11.419/2006.

PEDRO DE FIGUEIRÊDO LIMA NETO
CHEFE DA SEÇÃO DE INFRA-ESTRUTURA DE REDES

Documento assinado eletronicamente por PEDRO DE FIGUEIRÊDO LIMA NETO em 22/10/2020, às 13:38, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-pb.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0893556** e o código CRC **9D8D39F7**.

PODER JUDICIÁRIO
TRIBUNAL REGIONAL ELEITORAL DO AMAZONAS

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, 36 (trinta e seis) 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 36 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 36 meses ou de licença perpetua com suporte de 36 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.	0	50	R$ 1250,00	R$ 0,00
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.	0	50	R$ 1000,00	R$ 0.000,00
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.	0	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 250 endereços IP, por 36 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 5 domínios (FQDN), por 36 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.	0	50	R$ 1000,00	R$ 0,00

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 250 endereços IP, por 36 meses de uso e suporte do fabricante.	1	1	R$ 145.650,96	R$ 145.650,96
6.1.3-03	Tenable (on premise)	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$ 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.	0	50	R$ 0,00	R$ 0,00
6.1.3	Tenable (on premise)	----------	----------	----------	----------	R$ 165.314,00

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 36 meses ou de licença perpetua com suporte de 36 meses.

Valor Estimado (baseado na melhor proposta da Tenable on premise):
R$ 165.314,00 (Cento e sessenta 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 36 meses ou 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

TRIBUNAL REGIONAL ELEITORAL DO PIAUÍ
Praça Desembargador Edgard Nogueira. S/Nº - Centro Civico - Bairro Cabral - CEP 64000920 - Teresina - PI

ESTUDOS TÉCNICOS / 2020 - CODIN

1. IDENTIFICAÇÃO DA SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO

SOLUÇÃO DE TI	
NOME DA SOLUÇÃO DE TI:	Aquisição de solução de gestão de vulnerabilidades
ÁREA DEMANDANTE:	Coordenadoria de Desenvolvimento e Infraestrutura
E-MAIL DO DEMANDANTE:	antonio.sousa@tre-pi.jus.br
TELEFONE DO DEMANDANTE:	(86) 2107-9762

2. DESCRIÇÃO DA SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO

Contratação de solução de gestão de vulnerabilidades de segurança nos ativos de TI, serviços e sistemas de TI que rodam no ambiente web.

3. MOTIVAÇÃO / JUSTIFICATIVA

A dependência dos processos por recursos de tecnologia da informação aumenta a cada dia, fato do qual o setor governamental não é uma exceção.

Isso eleva a criticidade dos ativos de TI, sejam eles dados/informações, software ou hardware. Qualquer ativo que represente valor para a organização deve ser protegido contra vulnerabilidades que o torne indisponível, a exemplo do ocorrido com o STJ; que permita o vazamento de informações críticas ou mesmo que venha a afetar a imagem da organização.

Para isso, faz-se necessário que a Equipe de Tratamento de Incidentes de Rede realize suas atividades de forma pró-ativa e não apenas reativa.

Devido à complexidade da infraestrutura das organizações, a proteção aos ativos só é possível através de ferramentas automatizadas que permitam o monitoramento das vulnerabilidades de segurança antes que estas vulnerabilidades sejam exploradas.

Assim, faz-se necessária a aquisição de solução de gestão de vulnerabilidades que permita testar os ativos de TI e as aplicações web periodicamente em busca de quaisquer brechas, sejam elas relativas a atualização de sistemas operacionais e servidores de aplicação, configurações de serviços ou outras falhas técnicas. Além de fornecer dados atualizados à Alta Gestão acerca da segurança da informação da organização.

4. RESULTADOS ESPERADOS

A solução de software deve ser 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.

5. REQUISITOS DE NEGÓCIO

5.1 – Requisitos funcionais (Necessidades de negócio)

NECESSIDADE 1				
Gerenciamento de Vulnerabilidades em Sistemas Operacionais				
ID	**FUNCIONALIDADE**	**ID**	**RESPONSÁVEL**	**ÁREA**
1	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	1	Carlos Alberto Ribeiro do Nascimento Junior	SEINF
		...		
...				

NECESSIDADE 2				
Emissões de Relatórios				
ID	**FUNCIONALIDADE**	**ID**	**RESPONSÁVEL**	**ÁREA**
1	Emitir relatórios de acompanhamento dos testes e das vulnerabilidades encontradas, apontando quando forem solucionadas	1	Carlos Alberto Ribeiro do Nascimento Junior	SEINF

		...		
...				

5.2 – Requisitos não-funcionais

ID	TIPO	REQUISITO
1	Requisitos de capacitação	A contratação deve possuir um item de repasse tecnológico com no mínimo 20 horas para capacitar os servidores da STI a operacionalizar a ferramenta.
2	Requisitos Legais	Não há
3	Requisitos de Manutenção	Não há requisitos de manutenção dos itens adquiridos, exceto quando houver mudança de versão do sistema operacional.
4	Requisito Temporal	5.2.4.1. Prazos 5.2.4.1.1. O licitante terá 5 (cinco) dias contados da assinatura do contrato para fornecer os softwares ou as subscrições contratadas; 5.2.4.1.2. O atraso não justificado deverá ser punido de acordo com as sanções aplicadas ao contrato.
5	Requisitos de Segurança da Informação	5.2.5.1. 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 da Paraíba aos quais tiver acesso em decorrência do objeto da presente contratação, ficando terminantemente proibida de fazer uso ou revelação destes sob qualquer justificativa; 5.2.5.2. O Tribunal Regional Eleitoral da Piauí terá propriedade sobre todos os documentos e procedimentos operacionais produzidos no escopo da presente contratação; 5.2.5.3. Os documentos eventualmente produzidos deverão ser repassados ao Tribunal tanto em formato não editável (PDF) como também em formato editável (.DOCX). 5.2.5.4. 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.
6	Requisitos Sociais, Ambientais e Culturais	5.2.6.1. Logística Reversa 5.2.6.1.1. 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; 5.2.6.1.2. 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; 5.2.6.1.3. 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.
7	Requisitos de Desempenho	

5.3 – Requisitos tecnológicos

ID	TIPO	REQUISITO
1	Requisitos da Arquitetura Tecnológica	5.3.1.1. 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; 5.3.1.2. A solução deve possuir recurso de varredura ativa, onde o scanner comunica-se com os alvos (ativos) através da rede; 5.3.1.3. A solução de gestão de vulnerabilidades deve suportar varreduras de dispositivos de IoT; 5.3.1.4. Deve ser capaz de identificar no mínimo 50.000 CVEs (Common Vulnerabilities and Exposures); 5.3.1.5. 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; 5.3.1.6. Deve atribuir a todas as vulnerabilidades uma severidade baseada no CVSSv3 score; 5.3.1.7. 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; 5.3.1.8. A solução deve fornecer criptografia de ponta a ponta dos dados de vulnerabilidades; 5.3.1.9. A solução deve possuir a capacidade de armazenar informações dos ativos descobertos no ambiente; 5.3.1.10. Deve possuir um sistema de busca de informações de um determinado ativo com no mínimos as seguintes características:

5.3.1.10.1. Por sistema operacional;
5.3.1.10.2. Por um determinado software instalado;
5.3.1.10.3. Por Ativos impactados por uma determinada vulnerabilidade.
5.3.1.11. A solução deve possuir suporte para a adição de detecções personalizadas usando o OVAL (Open Vulnerability Assessment Language);
5.3.1.12. Deve permitir aceitar o risco de uma determinada vulnerabilidade encontrada no ambiente;
5.3.1.13. Possibilitar alterar a criticidade de determinada vulnerabilidade de forma manual;
5.3.1.14. A solução deve possuir um sistema de pontuação e priorização das vulnerabilidades;
5.3.1.15. A solução deve ser capaz de aplicar algoritmos de aprendizagem de máquina (machine learning) para analisar as características relacionadas a vulnerabilidades;
5.3.1.16. O sistema de pontuação e priorização de vulnerabilidades deve avaliar no mínimo as seguintes características:
5.3.1.16.1. CVSSv3 Impact Score;
5.3.1.16.2. Idade da Vulnerabilidade;
5.3.1.16.3. Se existe ameaça ou exploit que explore a vulnerabilidade;
5.3.1.16.4. Número de produtos afetados pela vulnerabilidade;
5.3.1.17. Deve ser capaz de fazer a correlação em tempo real de ameaças ativas contra vulnerabilidades encontradas, incluindo feeds de inteligência de ameaças ao vivo;

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

5.3.1.19. 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;

5.3.1.20. A solução deve permitir a instalação de agentes em estações de trabalho e servidores, para varredura diretamente no sistema operacional;
5.3.1.21. 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.

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

5.3.1.25. 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;

5.3.1.26. Deve ser possível determinar em tempo real quais portas de serviços (UDP/TCP) estão abertas em determinado ativo;
5.3.1.27. 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;
5.3.1.28. A solução deve ser capaz de em tempo real detectar logins e downloads de arquivos em um compartilhamento de rede;

5.3.1.29. Permitir identificar vulnerabilidades associadas a servidores SQL no tráfego de rede;
5.3.1.30. A solução deve possuir interface para integração com as principais soluções de SIEM de mercado, tais como IBM QRadar, Microfocus ArcSight e Splunk.
5.3.1.31. 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.
5.3.1.32. A atualização das ameaças deve ocorrer diariamente e sem interrupção dos serviços.

5.3.1.33. 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).

5.3.1.34. Todas as licenças de uso de software devem ser registradas, na data da entrega, em nome da Contratante no site do fabricante.
5.3.1.35. Dos Relatórios:
5.3.1.35.1. Deve ser capaz de executar relatórios periódicos de acordo com a frequência estabelecida pelo administrador, bem como a geração de relatórios sob demanda;
5.3.1.35.2. A solução deve possibilitar a criação de relatórios baseados na seleção de ativos, permitindo inclusive a seleção de todos os ativos existentes;
5.3.1.35.3. Deve suportar a criação de relatórios criptografados (protegidos por senha configurável) ;
5.3.1.35.4. A solução deve suportar o envio automático de relatórios para destinatários específicos;
5.3.1.35.5. Deve ser possível definir a frequência na geração dos relatórios para no mínimo: Diário, Mensal, Semanal e Anual;
5.3.1.35.6. Permitir especificar níveis de permissão nos relatórios para usuários e grupos específicos;
5.3.1.35.7. A solução deve fornecer relatórios do tipo “scorecard” para as partes interessadas da empresa;
5.3.1.35.8. A solução deve fornecer relatórios de correções aplicadas, classificados pelos seguintes critérios: grupo de ativos, usuários e vulnerabilidades;
5.3.1.36. A solução deve permitir mecanismo de varredura baseado em inferência com técnicas de varredura não intrusivas;
5.3.1.37. A solução deve possuir ou permitir a criação de relatórios com as seguintes informações:
5.3.1.37.1. Hosts verificados sem credenciais;
5.3.1.37.2. Top 100 Vulnerabilidades mais criticas;
5.3.1.37.3. Top 10 Hosts infectados por Malwares;
5.3.1.37.4. Hosts exploráveis por Malwares;
5.3.1.37.5. Total de vulnerabilidades que podem ser exploradas pelo Metasploit;
5.3.1.37.6. Vulnerabilidades críticas e exploráveis;
5.3.1.37.7. Máquinas com vulnerabilidades que podem ser exploradas;
5.3.1.38. A solução deve possuir dashboards customizáveis onde o administrador pode criar, editar ou remover painéis de acordo com a necessidade;
5.3.1.39. A solução deve ser capaz de inventariar todos os ativos da rede local e publicados na Internet, sem limites de endereços IPs.
5.3.1.40. A plataforma de software deve ser capaz de realizar varreduras (scans) de vulnerabilidades para no mínimo 250 IPs;
5.3.1.41. A plataforma de software deve ser licenciada para um número ilimitado de scanners (prevendo redundância);
5.3.1.42. Deve permitir a configuração de vários painéis e widgets;
5.3.1.43. Deve ser capaz de medir e reportar ameaças;
5.3.1.44. Deve ser capaz de visualizar ameaças críticas ao ambiente monitorado;
5.3.1.45. 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;
5.3.1.46. A plataforma de software deve suportar vários mecanismos de varredura distribuídos em diferentes localidades e regiões e gerenciar todos por uma console central;
5.3.1.47. 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;
5.3.1.48. A plataforma de software deve permitir o monitoramento através de agentes instalados, até o limite de licenças adquiridas, para varredura diretamente no sistema operacional.

5.3.1.49. 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.
5.3.1.50. 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;
5.3.1.51. 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;
5.3.1.52. A plataforma de software deve ser configurável para permitir a otimização das parametrizações de varredura;
5.3.1.53. 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;
5.3.1.54. A plataforma de software deve fornecer a capacidade de escalar privilégios nos destinos, do acesso de usuário padrão até acesso de sistema ou administrativo;
5.3.1.55. A plataforma de software deve ser capaz de realizar pesquisas de dados confidenciais;

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

5.3.1.56.1 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:

5.3.1.56.2. A solução de análise deve ser capaz de analisar, testar e reportar falhas de segurança em aplicações Web;
5.3.1.56.3. A solução de análise deverá ser capaz de executar varreduras em sistemas Web através de seus endereços IP ou FQDN (DNS);
5.3.1.56.4. A solução de análise deve ser capaz de identificar vulnerabilidades de divulgação de dados, como vazamento de informações de identificação pessoal;
5.3.1.56.5. 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;
5.3.1.56.6. Deverá também permitir a execução da função crawler, que consiste na navegação para descoberta das URLs existentes na aplicação;
5.3.1.56.7. A solução de análise deve suportar a integração com o softwares de automação de testes para permitir sequências de autenticação complexas;
5.3.1.56.8. A solução de análise deve ser capaz de realizar testes/varreduras em aplicações separadas, simultaneamente limitadas ao número de licenças;
5.3.1.56.9. A solução de análise deve oferecer suporte à capacidade de testar novamente a vulnerabilidade específica que foi detectada anteriormente no aplicativo Web;
5.3.1.56.10. Deve ser capaz de utilizar scripts customizados de crawling com parâmetros definidos pelo usuário;
5.3.1.56.11. Deve ser capaz de excluir determinadas URLs da varredura através de expressões regulares;
5.3.1.56.12. Deve ser capaz de excluir determinados tipos de arquivos através de suas extensões;
5.3.1.56.13. 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;
5.3.1.56.14. Deve ser capaz de agendar a varredura e determinar sua frequência entre uma única vez, diária, semanal, mensal e anual;
5.3.1.56.15. Deve suportar o envio de notificações por email;
5.3.1.56.16. Deverá ser compatível com avaliação de web services REST e SOAP;
5.3.1.56.17. A solução de análise deve suportar os seguintes esquemas de autenticação:
a) Autenticação Básica (Digest);
b) NTLM;
c) Autenticação de Cookies;
5.3.1.56.18. Deve ser capaz de importar scripts de autenticação previamente configurados pelo usuário;
5.3.1.56.19. 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;
5.3.1.56.20. Os resultados devem ser apresentados agregados por vulnerabilidades ou por aplicações;
5.3.1.56.21. Para cada vulnerabilidade encontrada, deve ser exibido detalhes e evidências;
5.3.1.56.22. Cada vulnerabilidade encontrada deve conter também soluções propostas para mitigação ou remediação;
5.3.1.56.23. 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.
5.3.1.56.24. 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.
2	Requisitos do Projeto de Implantação da solução de TI	
3	Requisitos da Garantia e Manutenção	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.
4	Requisitos de Capacitação	
5	Requisitos de Experiência Profissional da Equipe Técnica	
6	Requisitos de Formação da Equipe Técnica	
7	Requisitos da Metodologia de trabalho	
8	Requisitos de Segurança sob o ponto de vista Técnico	

5.4 – Outros requisitos

ID	TIPO	REQUISITO
1		
...		

6. IDENTIFICAÇÃO DAS SOLUÇÕES DISPONÍVEIS

SOLUÇÃO 1	**NOME DA SOLUÇÃO:**	Softwares livres OpenVas e Nmap
	DESCRIÇÃO:	Utilizar ferramentas livres ou gratuitas, como os softwares OpenVas e Nmap.
	FORNECEDOR(ES):	Comunidades Open Source e páginas específicas dos projetos.
	ENTIDADE:	
	VALOR:	0,00
SOLUÇÃO 2	**NOME DA SOLUÇÃO:**	Solução de Gestão de Vulnerabilidades On Cloud
	DESCRIÇÃO:	Aquisição de software de gerenciamento de vulnerabilidades e análise dinâmica de aplicações web baseado em nuvem, com modelo de subscrição por 60 meses.
	FORNECEDOR(ES):	Empresa: Service IT, Ferramenta: Qualys (1127024), proposta: **R$ 315.698,00;** Empresa: SERVIX, Tenable (1127028), proposta: **R$ 391.256,00;** e Empresa: Netconn,, Rapid7 (1127026), proposta: **R$ 716.112,50.** **Devido a grande disparidade de valor a proposta da empresa Netconn será desconsiderada.**
	ENTIDADE:	
	VALOR MÉDIO:	**R$ 353.477,00**
SOLUÇÃO 3	**NOME DA SOLUÇÃO:**	Solução de Gestão de Vulnerabilidades On premises
	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.
	FORNECEDOR(ES):	Empresa: SERVIX, Ferramenta:Tenable (1127028), proposta: **R$ 211.310,00** ; e

		Empresa: Netconn, Ferramenta: Rapid7 (1127026), proposta: **R$ 921.631,25** **Devido a grande disparidade de valor a proposta da empresa Netconn será desconsiderada.**
	ENTIDADE:	
	VALOR MÉDIO:	**R$ 211.310,00**

7. DETALHAMENTO DAS SOLUÇÕES E ALTERNATIVAS EXISTENTES

REQUISITO	ID DA SOLUÇÃO	SIM	NÃO	NÃO SE APLICA
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública Federal?	1			X
	2	X		
	3	X		
A Solução encontra-se implantada em outro órgão ou entidade da Justiça Eleitoral?	1			X
	2	X		
	3	X		
A Solução está disponível no Portal do Software Público Brasileiro?	1			X
	2			X
	3			X
A Solução é um software livre ou software público?	1	X		
	2		X	
	3		X	
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões e-PING, e-MAG?	1			X
	2			X
	3			X
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	1			X
	2			X
	3			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Judiciário – MoReq-Jus?	1			X
	2			X
	3			X

8. ANÁLISE E COMPARAÇÃO DOS CUSTOS TOTAIS DA DEMANDA

As pesquisas de preços constantes neste processo deram-se a partir de estudos e pesquisas conduzidos por alguns Tribunais da Justiça Eleitoral e é resultado de trabalho colaborativo destes Regionais. As propostas foram solicitadas para atender aos Tribunais que manifestaram interesse na aquisição de solução de gestão de vulnerabilidades.

Os custos estimados da contratação são conforme tabela abaixo.

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

COMPARAÇÃO DOS CUSTOS DAS PROPOSTAS ON CLOUD						
Item	Fornecedor	Descrição/Modelo	Quantidade Prevista	Quantidade Registrada	Valor Unitário	Valor Total
8.1	Comunidades	Softwares livres OpenVas e Nmap	0	0	R$ 0,00	R$ 0,00
8.2.1 - 02	Qualys (on cloud)	Licenciamento de plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando no mínimo 250 endereços IP, por 60 meses de uso e suporte do fabricante.	1	1	R$ 212.040,00	R$ 212.040,00

8.2.2.- 03	Qualys (on cloud)	Licenciamento para solução de análise dinâmica em aplicações Web, pacote para no mínimo 5 domínios (FQDN), por 60 meses de uso e suporte do fabricante.	1	1	R$ 92.268,00	R$ 92.268,00
8.2.3. - 04	Qualys (on cloud)	Instalação e configuração.	1	1	R$ 6.890,00	R$ 6.890,00
8.2.4. -05	Qualys (on cloud)	Repasse Tecnológico com período mínimo de 20 horas.	1	1	R$ 4.500,00	R$ 4.500,00
8.2.5. -06	Qualys (on cloud)	4 Horas de Serviço Especializado.	0	50	R$ 1250,00	R$ 0,00
8.2	**TOTAL Qualys (on cloud)**	----------	----------	----------	----------	**R$ 315.698,00**
8.3.1 -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 60 meses de uso e suporte do fabricante.	1	1	R$ 257.075,00	R$ 257.075,00
8.3.2 -03	Rapid7 (on cloud)	Licenciamento para solução de análise dinâmica em aplicações Web, pacote para no mínimo 5 domínios (FQDN), por 60 meses de uso e suporte do fabricante.	1	1	R$ 411.037,50	R$ 411.037,50
8.3.3 -04	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
8.3.4 -05	Rapid7 (on cloud)	Repasse Tecnológico com período mínimo de 20 horas.	1	1	R$ 10.000,00	R$ 10.000,00
8.3.5-06	Rapid7 (on cloud)	4 Horas de Serviço Especializado.	0	50	R$ 1000,00	R$ 0.000,00
8.3	**TOTAL Rapid7 (on cloud)**	----------	----------	----------	----------	**R$ 716.112,50**

8.4.1-02	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$ 263.742,00	R$ 263.742,00
8.4.2-03	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$ 107.850,00	R$ 107.850,00
8.4.3-04	Tenable (on cloud)	Instalação e configuração e repasse Tecnológico com período mínimo de 20 horas.	1	1	R$ 11.322,00	R$ 11.322,00
8.4.4-05	Tenable (on cloud)	Repasse Tecnológico com período mínimo de 20 horas	1	1	R$ 8.342,00	R$ 8.342,00
8.4.5-06	Tenable (on cloud)	4 Horas de Serviço Especializado.	0	50	R$ 0,00	R$ 0,00
8.4	**TOTAL Tenable (on cloud)**	----------	----------	----------	----------	**R$ 391.256,00**

COMPARAÇÃO DOS CUSTOS DAS PROPOSTAS ON PREMISES (LICENÇAS PERPÉTUAS)						
Item	Fornecedor	Descrição/Modelo	Quantidade Prevista	Quantidade Registrada	Valor Unitário	Valor Total
8.5.1-02	Rapid7 (on premise)	Licenciamento de plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando no mínimo 250 endereços IP, por 60 meses de uso e suporte do fabricante.	1	1	R$ 257.075,00	R$ 257.075,00
8.5.2-03	Rapid7 (on premise)	Licenciamento para solução de análise dinâmica em aplicações Web, pacote para no	1	1	R$ 123.311,25 por aplicação	R$ 616.556,25

		mínimo 5 domínios (FQDN), por 60 meses de uso e suporte do fabricante.				
8.5.3-04	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
8.5.4-05	Rapid7 (on premise)	Repasse Tecnológico com período mínimo de 20 horas.	1	1	R$ 10.000,00	R$ 10.000,00
8.5.5-06	Rapid7 (on premise)	4 Horas de Serviço Especializado.	0	50	R$ 1000,00	R$ 0,00
8.5	**TOTAL Rapid7 (on premise)**	----------	----------	----------	----------	**R$ 921.631,25**
8.6.1-02	Tenable (on premise)	Licenciamento de plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando no mínimo 250 endereços IP, por 60 meses de uso e suporte do fabricante.	1	1	R$ 191.646,00	R$ 191.646,00
8.6.2-03	Tenable (on premise)	Licenciamento para solução de análise dinâmica em aplicações Web, pacote para no mínimo 5 domínios (FQDN), por 60 meses de uso e suporte do fabricante.	1	1	R$ 0,00	R$ 0,00
8.6.3-04	Tenable (on premise)	Instalação e configuração.	1	1	R$ 11.322,00	R$ 11.322,00
8.6.4-05	Tenable (on premise)	Repasse Tecnológico com período mínimo de 20 horas	1	1	R$ 8.342,0	R$ 8.342,00
8.6.5-06	Tenable (on premise)	4 Horas de Serviço Especializado.	0	50	R$ 0,00	R$ 0,00
8.6	**Tenable (on premise)**	----------	----------	----------	----------	**R$ 211.310,00**

De forma resumida temos a tabela a seguir apresenta as propostas que estão sendo consideradas na análise dos custos:

Proposta	Empresa		

		Solução	Valor Total
COMPARAÇÃO DOS CUSTOS DAS PROPOSTAS ON CLOUD			
1	Service IT	Qualys	**R$ 315.698,00**
3	SERVIX	Tenable	**R$ 391.256,00**
COMPARAÇÃO DOS CUSTOS DAS PROPOSTAS ON PREMISES (LICENÇAS PERPÉTUAS)			
6	SERVIX	Tenable	**R$ 211.310,00**

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 uma nuvem na qual não temos o controle algum sobre acesso, armazenamento e segurança. O armazenamento de dados sensíveis em nuvem é ainda desaconselhado pela Norma Complementar 14 do Gabinete de Segurança Institucional da Presidência da República.**

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 à solução 3 fornecida pela Tenable é o fato de que após o término do suporte a STI 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.

Esclarecemos que inicialmente, manifestamos interesse em adquirir licenciamento para 250 IPs, por 3 anos de uso, mas ao final quando verificamos o preço oferecido pela empresa SERVIX Informática Ltda, que apresentou a solução Tenable, resolvemos requerer o licenciamento para 5 anos de uso.

9. SOLUÇÃO ESCOLHIDA

9.1 – Identificação

NOME:	Solução de Gestão de Vulnerabilidades On premises (licenças perpétuas)		
JUSTIFICATIVA:	A solução escolhida além de apresentar o menor preço permite ao Tribunal continuar utilizando a ferramenta adquirida após os 5 anos de uso, porém sem o direito de realizar atualizações de versão e de novas vulnerabilidades.		
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.		
BENS E SERVIÇOS	**ID**	**BEM / SERVIÇO**	**VALOR ESTIMADO**
	1	Licenciamento de plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando no mínimo 250 endereços IP, por 60 meses de uso e suporte do fabricante.	R$ 191.646,00
	2	Licenciamento para solução de análise dinâmica em aplicações Web, pacote para no mínimo 5 domínios (FQDN), por 60 meses de uso e suporte do fabricante.	0,00
	3	Instalação e configuração.	R$ 11.322,00
	4	Repasse Tecnológico com período mínimo de 20 horas	R$ 8.342,00
	5	4 Horas de Serviço Especializado.	0,00
	...	**TOTAL ESTIMADO:**	R$ 211.310,00

9.2 – Alinhamento com as necessidades de negócio

ID	FUNÇÃO	NECESSIDADE DO NEGÓCIO
1	A solução é capaz de identificar vulnerabilidades catalogadas em diversos CVEs (*Common Vulnerabilities and Exposures*)	Gerenciamento de vulnerabili Sistemas Operacionais
2	A solução é capaz de calcular a criticidade com base nos dados agregados e consolidados do ativo, dados de segurança, sistema e conformidade, bem como hierarquias e prioridades	Aumentar o nível da segurança da
3	A solução é capaz de gerar relatórios de acompanhamento para a Alta Gestão tomar conhecimento da evolução da gestão de	Emissões de relatórios

	vulnerabilidades do órgão

9.3 – Benefícios esperados

ID	TIPO	BENEFÍCIOS
1	Conformidade	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.
2	Confiabilidade	Utilização de ferramentas atualizadas contra ameaças cibernéticas
3	Disponibilidade	A eliminação de vulnerabilidades propiciará à rede do TRE-PI uma maior imunidade à ataques cibernéticos, aumentando sua resiliência e disponibilidade
4	Segurança	A eliminação de vulnerabilidades propiciará uma maior segurança dos dados e ativos do Tribunal
5	Padronização	Utilização de solução utilizada pelo TSE e TREs, possibilitando a troca de experiências
6	Orçamentária	Aquisição de solução com preço mais competitivo devido a compra em escala

9.4 – Justificativa de não-conformidade

ID	SOLUÇÃO	JUSTIFICATIVA
1	Softwares livres OpenVas e Nmap	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
2	Solução de Gestão de Vulnerabilidades On Cloud	O armazenamento de dados sensíveis em nuvem é desaconselhado pela Norma Complementar 14 do Gabinete de Segurança Institucional da Presidência da República.

10. AVALIAÇÃO DAS NECESSIDADES DE ADEQUAÇÃO PARA EXECUÇÃO CONTRATUAL

ID	TIPO DE NECESSIDADE	SIM	NÃO	DESCRIÇÃO
1	Infraestrutura Tecnológica		X	
2	Infraestrutura Elétrica		X	
3	Logística de implantação	X		Disponibilizar mão de obra especializada para implantação da solução e testes de configuração necessárias ao seu bom funcionamento.
4	Espaço Físico		X	
5	Mobiliário		X	
6	Impacto ambiental		X	

11. RECURSOS NECESSÁRIOS À CONTINUIDADE DO NEGÓCIO DURANTE E APÓS A EXECUÇÃO DO CONTRATO

DESCRIÇÃO DOS RECURSOS NECESSÁRIOS PARA SUPORTAR A CONTRATAÇÃO DA SOLUÇÃO		
11.1. Recursos Materiais		
Item	**Descrição**	
1	Não se aplica	
...		
11.2. Recursos Humanos		
Item	**Função**	**Formação**
1	Administrador de Redes	Conhecimento em configuração da rede de computares e segurança da informação
...		

12. ESTRATÉGICA DE CONTINUIDADE CONTRATUAL

IDENTIFICAÇÃO DE EVENTOS QUE POSSAM CAUSAR INTERRUPÇÃO CONTRATUAL			
Evento	**Descrição**	**Ação de Contingência**	**Responsável**
1	Não entregar ou entregar o objeto fora do prazo estabelecido durante a contratação.	Multa / Considerar inexecução parcial ou total do objeto	SAOF
2	Em garantia, corrigir ou substituir o objeto fora do prazo estabelecido	Multa / Considerar inexecução parcial ou total do objeto	SAOF
3	Em garantia, não fornecer as atualizações necessárias ao bom funcionamento da solução	Multa / Considerar inexecução parcial ou total do objeto	SAOF

13. AÇÕES PARA TRANSIÇÃO E ENCERRAMENTO CONTRATUAL

Item	Ação	Responsável	Data Início	Data Fim
1	Os requisitos de negócio e os serviços de suporte serão cobertos pela garantia previstas no Termo de Referência. Durante esse período, a contratada será obrigada a fornecer todas as atualizações necessárias e manter os serviços ativos. No mínimo 180 (cento e oitenta) dias antes do encerramento do Contrato, será iniciado novo procedimento licitatório para substituição e/ou continuidade dos serviços da solução.	CODIN	01/06/2025	01/01/2026
...				

14. ESTRATÉGIA DE INDEPENDÊNCIA

14.1. Transferência de Conhecimento Tecnológico		
Item	**Informações que deverão ser transmitidas pela Contratada**	**Forma de transferência do Conhecimento**
1	Formas de instalação, desinstalação e operacionalização	Treinamento
2	Resolução de inconsistências, dúvidas e adequações	Suporte
14.2. Direitos de Propriedade Intelectual e Autorais		
Item	**Cláusulas segundo a lei Nº 9.610, de 19 de fevereiro de 1998.**	
1	Não se aplica	
...		

15. ANÁLISE DE RISCOS

15.1 – Riscos do processo de contratação (identificar os riscos que podem comprometer o processo de contratação, resultando em atrasos ou em comprometimento do processo de contratação – IN04, art. 16, I)

RISCO 1					**PROBABILIDADE**	
Tempo excessivo na tramitação do processo de adesão					( ) 1-Baixo ( ) 2-Médio (X) 3-Alto ( ) 4-Muito alto	
ID	**EFEITO**	**IMPACTO**	**AÇÃO DE RESPOSTA AO RISCO**	**TIPO DE AÇÃO**	**RESPONSÁVEL**	**ÁREA**
1	Impossibilidade de participação na IRP do TRE-PB	( ) 1-Baixo ( ) 2-Médio (X) 3-Alto ( ) 4-Muito alto	Realizar contratação própria	( ) 1-Mitigação (X) 2-Contingência	Integrante Demandante	CODIN
2	Maior custo para contratação da solução	( ) 1-Baixo ( ) 2-Médio (X) 3-Alto ( ) 4-Muito alto	Solicitar suplementação orçamentária	( ) 1-Mitigação ( ) 2-Contingência	Integrante Demandante	CODIN

RISCO 2					**PROBABILIDADE**	
Não disponibilidade orçamentária para aquisição da solução escolhida					( ) 1-Baixo ( ) 2-Médio (X) 3-Alto ( ) 4-Muito alto	
ID	**EFEITO**	**IMPACTO**	**AÇÃO DE RESPOSTA AO RISCO**	**TIPO DE AÇÃO**	**RESPONSÁVEL**	**ÁREA**
1	Não contratação	( ) 1-Baixo (X) 2-Médio ( ) 3-Alto ( ) 4-Muito alto	Remanejamento de recursos de outras aquisições menos prioritárias	( ) 1-Mitigação (X) 2-Contingência	Integrante Demandante Integrante Administrativo	CODIN SAOF
2	Deixar a rede do TRE-PI vulnerável à ameaças cibernéticas	( ) 1-Baixo ( ) 2-Médio ( ) 3-Alto (X) 4-Muito alto	Solicitação de Orçamento	(X) 1-Mitigação ( ) 2-Contingência	Integrante Demandante	CODIN
4	Utilização de ferramentas/recursos open source	( ) 1-Baixo (X) 2-Médio ( ) 3-Alto ( ) 4-Muito alto	Viabilizar outras camadas de segurança	( ) 1-Mitigação (X) 2-Contingência	Integrante Técnico	SEINF

15.2 – Riscos da solução de TI escolhida (identificar os riscos que podem fazer com que, após o serviço ter sido contratado, o mesmo não atenda às necessidades do negócio especificadas – IN04, art. 16, II)

RISCO 1					**PROBABILIDADE**	
Serviços de suporte/garantia de baixa qualidade					(X) 1-Baixo ( ) 2-Médio ( ) 3-Alto ( ) 4-Muito alto	
ID	**DANO**	**IMPACTO**	**AÇÃO DE RESPOSTA AO RISCO**	**TIPO DE AÇÃO**	**RESPONSÁVEL**	**ÁREA**
1	Solução funcionando inadequadamente ou base de vulnerabilidades desatualizada	( ) 1-Baixo ( ) 2-Médio (X) 3-Alto ( ) 4-Muito alto	Acompanhar abertura de chamado e sugerir aplicação de multa à contratada, caso os prazos estabelecidos em edital não sejam atendidos	(X) 1-Mitigação ( ) 2-Contingência	Fiscal Técnico/Administrativo	SEINF

RISCO 2					**PROBABILIDADE**	
O software e produtos contratados não atendem completamente aos requisitos propostos para a aquisição					(X) 1-Baixo ( ) 2-Médio ( ) 3-Alto ( ) 4-Muito alto	
ID	**EFEITO**	**IMPACTO**	**AÇÃO DE RESPOSTA AO RISCO**	**TIPO DE AÇÃO**	**RESPONSÁVEL**	**ÁREA**
1	Não atendimento as demandas do negócio	( ) 1-Baixo ( ) 2-Médio (X) 3-Alto ( ) 4-Muito alto	Realização de prova de conceito da ferramenta antes de adquirir	(X) 1-Mitigação ( ) 2-Contingência	Integrante Técnico	SEINF

16. ESTRATÉGIA PARA CONTRATAÇÃO

16.1. SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (Res. CNJ 182/2013, art. 16)

16.1.1 – DEFINIÇÃO (NATUREZA DO OBJETO) DA SOLUÇÃO (critérios que serão usados para definir o tipo de contratação, modalidade de licitação, etc: inovação tecnológica ou serviço/bem comum; necessidade pontual ou contínua- Res. CNJ 182/2013, art. 16, IV)	
Critério	**Atendimento da Solução**
É possível especificar o serviço usando parâmetros usuais de mercado?	Sim
É possível medir o desempenho da qualidade usando parâmetros usuais de mercado?	Sim
O objeto da contratação se estende necessariamente por mais de um ano?	Sim.
O objeto da contratação é essencial para o negócio?	Sim. A solução visa gerenciar as vulnerabilidades de ativos que se forem exploradas por hackers poderá inviabilizar o acesso aos serviços e sistemas de TI críticos pra o negócio.

16.1.2 – PARCELAMENTO E ADJUDICAÇÃO DA CONTRATAÇÃO (justificar se é técnica e economicamente viável dividir a solução a ser contratada. Informar se o objeto pode ou não ser dividido em itens ou até mesmo em grupos. Em caso de divisão, verificar se há prejuízo nos resultados finais a serem obtidos. De acordo com o parcelamento do objeto, informar se a adjudicação pode ou não ser realizada para mais de um fornecedor. Justificar a escolha. Esse item não se aplica aos casos de Dispensa ou Inexigibilidade - (Res. CNJ 182/2013, art. 16, II e III)
A solução não é divisível, uma vez que é composta por elementos interdependentes, administrados coletivamente por uma única console central de gerenciamento.

16.2. RESPONSABILIDADES DA CONTRATANTE E DA CONTRATADA

16.2.1 – DEVERES E RESPONSABILIDADES DA CONTRATANTE (deveres e responsabilidades da contratante que comporão o contrato)	
ID	**Dever / Responsabilidade**
1	16.2.1.1. Prestar informações e esclarecimentos que venham a ser solicitados pela CONTRATADA, necessários à execução do contratado;

	16.2.1.2. Notificar a Contratada por escrito da ocorrência de eventuais imperfeições dos equipamentos, fixando prazo para a sua correção de acordo com os definidos no presente Termo; 16.2.1.3. Verificar se os equipamentos estão de acordo com as especificações, podendo sustar, recusar, mandar fazer ou desfazer qualquer serviço que esteja em desacordo com as especificações deste documento; 16.2.1.4. Atestar a(s) notas fiscal(ais) apresentada(s) pela CONTRATADA após o recebimento definitivo dos equipamentos, conforme especificações descritas neste Termo de Referência; 16.2.1.5. Efetuar o pagamento nas condições, preços e prazos pactuados; 16.2.1.6. Acompanhar e fiscalizar o cumprimento das obrigações da contratada, determinando o que for necessário a regularização das falhas ou defeitos observados, ou ainda propor aplicações de penalidades e a sanções administrativas regulamentares e contratuais cabíveis, sempre que for o caso.

16.2.2 – DEVERES E RESPONSABILIDADES DA(S) CONTRATADA(S) (deveres e responsabilidades da(s) contratada(s) que comporão o contrato. A(s) contratada(s) não poderá(ão) se eximir dessas responsabilidades, mesmo havendo subcontratação - (IN04, art. 15, II)

ID	Dever / Responsabilidade
1	2.2.1. A Contratada deve cumprir todas as obrigações constantes no Edital, seus anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto e, ainda: a) Efetuar a entrega do objeto em perfeitas condições, conforme especificações, prazo e local constantes no Edital e seus anexos. b) Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, as partes do objeto deste contrato em que se verificarem vícios, defeitos ou incorreções resultantes dos materiais empregados. c) Deverá guardar sigilo sobre dados e informações obtidos em razão da execução dos serviços contratados ou da relação contratual mantida com o TRE-PI, abstendo-se de divulgá-los a terceiros sob qualquer pretexto, a menos que prévia e formalmente autorizado pelo TRE-PI. d) Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, de acordo com os artigos 14 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990), ficando a Contratante autorizada a descontar dos pagamentos devidos à Contratada, o valor correspondente aos danos sofridos; 2.2.2. A CONTRATADA deverá respeitar as normas de segurança estabelecidas pela CONTRATANTE durante a realização de atividades no ambiente desta. 2.2.3. A CONTRATADA deverá: a) prover assistência técnica no **território** brasileiro; b) dispor de um número telefônico para suporte técnico e abertura de chamados técnicos, c) apresentar tempo de resposta aos chamados abertos em até no máximo 6 horas; d) possuir um sistema de atendimento de suporte via Chat, 0800 ou através da Internet; **e) dar garantia não inferior a 60 meses, a contar da data de emissão do Termo de Recebimento Definitivo;** 2.2.4. Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

16.3 INDICAÇÃO DOS TERMOS CONTRATUAIS (IN04, art. 15, III)

16.3.1 – PROCEDIMENTOS E CRITÉRIOS DE ACEITAÇÃO (IN04, art. 15, III, a)

ID	**Etapa / Fase / Item** (em qual etapa, fase ou item do projeto será aplicada a mensuração)	**Indicador** (qual será o indicador mensurado. Qual será a unidade de medida a ser avaliada)	**Valor Mínimo Aceitável** (valor mínimo aceitável daquele item de mensuração)
1	Aceitação da proposta	Configurações dos equipamentos/serviços ofertados	Valores mínimos exigidos no Edital.
...			

16.3.2 – FORMA DE PAGAMENTO (modo ou percentual que será pago por cada entrega em função do resultado a ser obtido -IN04, art. 15, III, e)

O pagamento será efetuado por meio de depósito bancário em conta corrente, até o 10º (décimo) dia útil a partir da apresentação da Fatura/Nota Fiscal, devidamente certificada pelo fiscal do contrato e processada na forma da legislação vigente.

16.3.3 – CRONOGRAMA DE EXECUÇÃO FÍSICO-FINANCEIRA (IN04, art. 15, III, f)

ID	**Entrega** (listagem do item ou serviço a ser entregue. Esta entrega pode ser parcelada ou integral)	Data de Entrega	Percentual a ser Pago
1	Solução para Gestão de vulnerabilidades on premises	Até 05(cinco) dias contados da assinatura do contrato	100%

...			
Total: R$ 211.310,00			

16.3.4 – MECANISMOS FORMAIS DE COMUNICAÇÃO (IN04, art. 15, III, g)				
Função de Com. 1 (listagem do que deverá ser contemplado neste mecanismo de comunicação):	Assinatura de contrato, emissão de ordem de fornecimento, emissão de notas fiscais.			
Documento (nome do documento a ser entregue)	**Emissor**	**Destinatário**	**Meio** (forma com que o documento deverá ser produzido e entregue)	**Periodicidade** (frequência que os documentos deverão ser emitidos e entregues pela contratada ou pela administração)
Ata de Registro de Preços	Contratante	Contratada	Eletrônico	1 vez
Contrato	Contratante	Contratada	Eletrônico	1 vez
Ordem de Fornecimento	Contratante	Contratada	Eletrônico	1 vez
Nota Fiscal	Contratante	Contratada	Físico/Eletrônico	1 vez
Nota de Empenho	Contratante	Contratada	Eletrônico	1 vez

16.3.5 – REGRAS PARA APLICAÇÃO DE MULTAS E SANÇÕES (IN04, art. 15, III, h)		
ID	**Ocorrência** (descrição clara das situações em que se caracterizará a infração a algum termo contratual. Devem ser descritas as não conformidades, ou outras situações ou ocorrências em que serão propostas sanções a serem aplicadas pela Área Administrativa)	**Sanção / Multa** (descrição da sanção/multa a ser aplicada de acordo com cada situação ou ocorrência listada. As multas e sanções devem ser proporcionais ao impacto que a ocorrência provocará no órgão e aos casos de reincidência das ocorrências)
1	• Não assinar o contrato ou Ata de Registro de Preços • Deixar de entregar documentação exigida neste edital; • Apresentar documentação falsa; • Não manter a proposta; • Falhar ou fraudar na execução do contrato; • Comportar-se de modo inidôneo; • Fazer declaração falsa; • Cometer fraude fiscal.	Fundamentado no artigo 7º da Lei 10.520/2002, regulamentado pelo artigo 49 do Decreto n.º 10.024/2019, ficará impedido de licitar e contratar com a União e será descredenciado no SICAF, pelo prazo de até 05 (cinco) anos, garantido o direito à ampla defesa
2	Faltas leves, assim entendidas aquelas que não acarretem prejuízos significativos para a Contratante	Penalidade de advertência
3	• Atraso no cumprimento das obrigações assumidas contratualmente, que tenha acarretado prejuízos financeiros para o TRE-PI; • Entrega de objeto, em desacordo com a proposta aceita pela Contratante, sem prejuízo das demais sanções.	Suspensão temporária de participação em licitação e impedimento de contratar com o TRE-PI, p**or até 1 (um) ano,** se, por culpa ou dolo, prejudicar ou tentar prejudicar a execução do Contrato
4	• Entrega de objeto falso, seja como amostra ou como bem a ser entregue por ocasião de emissão de ordem de fornecimento, assim entendido, aquele em que houve manipulação para aparentar ser de outra marca/fabricante, ou ter características que originalmente não lhe pertençam, sem prejuízo das demais medidas cabíveis; • Não atendimento à solicitação de troca ou prestação de garantia do objeto, quando solicitado pela Contratante, no prazo fixado no edital • Cometimento de quaisquer outras irregularidades que acarretem prejuízo ao TRE-PI, ensejando a rescisão do Contrato por culpa da CONTRATADA; • Apresentação, ao TRE-PI, de qualquer documento falso ou falsificado, no todo ou em parte, com o objetivo de comprovar, durante a execução do Contrato, a manutenção das condições apresentadas na habilitação	Suspensão temporária de participação em licitação e impedimento de contratar com o TRE-PI, p**or até 2 (dois) anos,** se, por culpa ou dolo, prejudicar ou tentar prejudicar a execução do Contrato
5	Entrega do objeto com atraso	Multa moratória mensurada na forma de tabela a ser prevista no termo de referência, até o limite de 13% (treze por cento), calculada sobre o valor do objeto em atraso.

6	Inexecução total do contrato	Multa compensatória de 15% (quinze por cento) sobre o valor do objeto

16.4. CRITÉRIOS TÉCNICOS DE JULGAMENTO DAS PROPOSTAS (IN04, art. 15, VII)

16.4.1 – CRITÉRIOS DE SELEÇÃO			
( ) Licitação (X) Registro de Preço ( ) Dispensa de licitação ( ) Inexigibilidade de licitação			
Modalidade:	Licitação	**Tipo:**	Pregão Eletrônico
Justificativa: (obrigatório se for dispensa ou inexigibilidade de licitação)	Aquisição de bens e/ou serviços comuns pelo Sistema de Registro de Preços devido a contratação não ter sido contemplada com o orçamento necessário para o exercício 2020. Dessa forma, mais benéfico ao Tribunal, participar de Intenção de Registro de Preços proposta pelo TRE-PB de forma a lhe possibilitar a aquisição por um custo menor.		

16.5. INDICAÇÃO DA EQUIPE DE GESTÃO DA CONTRATAÇÃO (ou comissão de recebimento de bens) (Res. CNJ 182/2013, art. 16, VIII)

Gestor do Contrato:	Antônio Manoel Silveira de Sousa	Telefone:	2107-9762
E-mail do Gestor do Contrato:	antonio.sousa@tre-pi.jus.br	Setor:	STI/CODIN
Fiscal Demandante:	Antônio Manoel Silveira de Sousa	Telefone:	2107-9762
E-mail do Fiscal Demandante:	antonio.sousa@tre-pi.jus.br	Setor:	STI/CODIN
Fiscal Técnico:	Carlos Alberto ribeiro do Nascimento Jr.	Telefone:	2107-9756
E-mail do Fiscal Técnico:	carlos.nascimento@tre-pi.jus.br	Setor:	STI/CODIN/SEINF
Fiscal Administrativo:	Sidnei Antunes Ribeiro	Telefone:	2107-9676
E-mail do Fiscal Administrativo:	sidnei.antunes@tre-pi.jus.br	Setor:	SAOF/COCONP/SELIC

17. ASSINATURAS

INTEGRANTE	NOME	ÁREA
Demandante:	Antônio Manoel Silveira de Sousa	STI/CODIN
Técnico:	Carlos Alberto ribeiro do Nascimento Jr.	STI/CODIN/SEINF
Administrativo:	Sidnei Antunes Ribeiro	SAOF/COCONP/SELIC

Teresina, 20 de novembro de 2020.

Documento assinado eletronicamente por **Carlos Alberto Ribeiro do Nascimento Junior**, **Técnico Judiciário**, em 23/11/2020, às 10:43, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Sidnei Antunes Ribeiro**, **Chefe de Seção**, em 23/11/2020, às 12:57, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Antonio Manoel Silveira de Sousa**, **Coordenador de Desenvolvimento e Infraestrutura**, em 23/11/2020, às 13:22, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-pi.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1126906** e o código CRC **02CA6F98**.

ESTUDO TÉCNICO PRELIMINAR DE VIABILIDADE DE CONTRATAÇÃO

Aquisição de Solução de Tecnologia da Informação

Processo PAD nº 022 909/2020

Objeto do Estudo	Licenciamento de software de gestão de vulnerabilidades cibernéticas, com garantia do fabricante. Vigência: 60 (sessenta) meses
Versão do documento	1.0
Elaboração	Coordenadoria de Infraestrutura – COINT e Seção de Suporte Operacional e Segurança da Informação – SESIC
Equipe de Estudo da solução	Jonas de Araújo Luz Jr., Lauro Salmito Pinheiro e Ticiano do Nascimento Diniz
Equipe de Planejamento	Jonas de Araújo Luz Jr. e Lauro Salmito Pinheiro
Equipe de Gestão Técnica da contratação	Jonas de Araújo Luz Jr. e Ticiano do Nascimento Diniz
Aprovação	Carlos Antônio Sampaio de Melo *Secretário de Tecnologia da Informação*

Sumário

Análise de Viabilidade da Contratação

1. Nome da Solução de Tecnologia da Informação

1.1. Licenciamento de software de gestão de vulnerabilidades cibernéticas, com garantia do fabricante. Vigência por 60 (sessenta) meses.

2. Documento de Oficialização da Demanda (Res. CNJ 182/2013, Art. 12, § 5º)

O Documento de Oficialização da Demanda (DOD) consta no doc. PAD nº 195021/2020.

3. Objetivos da Contratação (Res. CNJ 182/2013, Art. 12, § 5º, I)

A presente contratação tem o objetivo de contratar licenciamento de solução de software de gestão de vulnerabilidades cibernéticas, com capacidade de detecção, identificação, monitoramento e auditoria de vulnerabilidades em hardware, software e respectivas configurações que representem risco à segurança da informação na infraestrutura tecnológica do TRE/CE.

3.1.1. Objetivos Estratégicos (Res. CNJ 182/2013, Art.12, § 5º, I)

Os objetivos estratégicos associados ao presente estudo são:

PEJECE 2015-2020 – Macrodesafio: Melhoria da Infraestrutura e Governança de TIC.

PETIC 2015-2020 – PERSPECTIVA: EXCELÊNCIA OPERACIONAL

OBJETIVO: Implantar a Política de Segurança da Informação

OBJETIVO: Garantir a disponibilidade dos serviços de TIC necessários às atividades da Justiça Eleitoral

OBJETIVO: Garantir a infraestrutura de TIC necessária às atividades da Justiça Eleitoral

PETIC 2015-2020 – PERSPECTIVA: ORIENTAÇÃO FUTURA

OBJETIVO: Implantar a gestão de continuidade dos serviços de TIC

OBJETIVO: Assegurar a estrutura e a força de trabalho de TIC apropriadas à consecução dos objetivos de TIC

PETIC 2015-2020 – PERSPECTIVA: CONTRIBUIÇÃO CORPORATIVA

OBJETIVO: Implantar boas práticas de governança de TIC

3.1.2. Motivação / Justificativa (Res. CNJ 182/2013, Art.12, § 5º, II)

A defesa cibernética institucional ganha cada vez mais importância essencial à medida que se estruturam e se organizam os grupos criminosos que buscam se beneficiar de ataques cibernéticos às instituições, sejam suas motivações de natureza política (ideológica ou econômica) ou financeiras. Com o advento da COVID-19 e a adoção crescente do teletrabalho, a rede de dados institucional precisa ser acessada remotamente, o que eleva o risco de ataques[1].

A construção de um sistema de defesa cibernética eficaz deve considerar a defesa em diversas camadas, não confiando em uma solução única (panaceia) e levando em conta os diversos elementos e componentes de sua infraestrutura tecnológica que podem apresentar vulnerabilidades, desde equipamentos e software até sua força de trabalho, as pessoas. É comum afirmar-se que o sistema de defesa é tão forte quanto seu elo mais fraco.

Neste contexto, o TRE/CE dispõe hoje das camadas de defesa mais tradicionais, a saber: software antivírus e rede de *firewalls*, que protegem as estações e o tráfego na rede de computadores do TRE/CE. Entretanto, como anteriormente exposto, a defesa cibernética deve ser construída em camadas, levando em conta as possíveis "superfícies de ataque" existentes na infraestrutura.

Adicionalmente, ao longo desta semana passada, veio a público a ocorrência de ataque hacker bem-sucedido ao Superior Tribunal de Justiça (STJ), realizado por meio de *ransomware*, conforme notícias publicadas na imprensa[2] e reportado nos grupos de trabalho técnicos. O incidente de segurança forçou aquele tribunal superior a paralisar, praticamente por completo, todas as suas atividades, que ainda não retornaram à normalidade.

Torna-se importante, assim, dentre outras iniciativas possíveis, que se tenha a capacidade de monitorar, identificar e tratar as vulnerabilidades existentes nos recursos computacionais – hardware ou software – utilizados na infraestrutura. Neste campo, o mercado apresenta soluções de "gestão de vulnerabilidades", algumas das quais, inclusive, utilizam inteligência artificial para detectar potenciais vulnerabilidades ainda não conhecidas ou publicadas, as chamadas *Zero-Day*[3].

---

1 Notícia: **2020 é um dos piores anos para a segurança digital, afirma pesquisa**. Documento nº 194 995/2020. Fonte: site Olhar Digital <https://olhardigital.com.br/fique_seguro/noticia/2020-e-um-dos-piores-anos-para-a-seguranca-digital-afirma-pesquisa/109 763>. Acesso em 08/11/2020.

2 Coletânea de notícias acerca da invasão hacker bem-sucedida que "sequestrou" os dados do STJ, obrigando-o a suspender seus serviços e prazos processuais. Documento PAD nº Documento nº 194 740/2020.

3 Artigo: **Zero-Day**. Fonte: Wikipedia <https://en.wikipedia.org/wiki/Zero-day_(computing)> Acesso em 09/11/2020

4. Análise de Viabilidade de Contratação (Res. CNJ 182/2013, Art. 14)

4.1. Definição e Especificação dos Requisitos da Demanda (Art. 14, I)

A solução de gestão de vulnerabilidades deve ser capaz de atender aos requisitos apresentados na Tabela 1, apresentada adiante.

Tabela 1: Requisitos da demanda

4.1.1. Necessidades de Negócio *Necessidade vinculada aos objetivos de negócio, para alcance de metas do órgão, ou a descrição de um problema que deve ser resolvido, já devidamente previsto no PDTIC.*		
ID	**Atores Envolvidos** *Lista dos responsáveis pelas demandas funcionais (nome/setor) para o controle do atendimento de requisitos de todas as áreas impactadas.*	
1	Jonas de Araújo Luz Junior	COINT
2	Ticiano do Nascimento Diniz	SESIC
Necessidade 1	**Software de gestão de vulnerabilidades.**	
ID	**Funcionalidade e Requisitos técnico-funcionais**	
1	**Gerenciamento de vulnerabilidades em sistemas operacionais.** Testar os servidores e estações de rede (físicos e virtuais) junto às bases de dados de vulnerabilidades mantidas por organizações especializadas em segurança da informação e por grandes fabricantes de software.	
2	**Gerenciamento de vulnerabilidades em sistemas e sítios web.** Testar as aplicações e sítios web, internos e externos, junto às bases de dados de vulnerabilidades mantidas por organizações especializadas em segurança da informação e por grandes fabricantes de software.	
3	**Emissão de relatórios gerenciais.** Emitir relatórios de acompanhamento dos testes e das vulnerabilidades encontradas, apontando quando forem solucionadas.	
4.1.2. Requisitos Tecnológicos (Res. CNJ nº 182/2013, art. 4º)		
ID	**Requisito**	
1	Funcionalidades de realizar varreduras de vulnerabilidades, avaliação de configuração e conformidade (*baseline* e *compliance*), indícios e padrões de códigos maliciosos conhecidos (*malware*) para, no mínimo, 350 (trezentos e cinquenta) IPs e 15 (quinze) domínios.	
2	**Varredura ativa**, onde o *scanner* comunica-se com os alvos (ativos) através da rede.	
3	Ser capaz de realizar varreduras de dispositivos de Internet das Coisas (IoT).	
4	Ser capaz de identificar, no mínimo, 50.000 CVEs (*Common Vulnerabilities and Exposures*).	
5	Capacidade de adicionar etiquetas (*tags*) aos ativos de maneira automática, manual e possibilitar o uso de regras com parâmetros específicos para aplicação das mesmas.	

4.1.2. Requisitos Tecnológicos (Res. CNJ nº 182/2013, art. 4º)	
ID	**Requisito**
6	Atribuir a todas as vulnerabilidades uma severidade baseada no CVSSv3 score.
7	Calcular a criticidade com base nos dados agregados e consolidados do ativo, dados de segurança, sistema e conformidade, bem como hierarquias e prioridades.
8	Fornecer criptografia de ponta a ponta dos dados de vulnerabilidades.
9	Ser capaz de armazenar informações dos ativos descobertos no ambiente.
10	Possuir mecanismo de busca de informações de ativos utilizando-se, ao menos, os seguintes parâmetros: • Sistema operacional; • Determinado software instalado; • Determinada vulnerabilidade que afete os ativos.
11	Possuir suporte para a adição de detecções personalizadas usando o OVAL (*Open Vulnerability Assessment Language*).
12	Aceitar o risco de uma determinada vulnerabilidade encontrada no ambiente.
13	Permitir se alterar a criticidade de determinada vulnerabilidade de forma manual.
14	Possuir um sistema de pontuação e priorização das vulnerabilidades, o qual deve avaliar, no mínimo, as seguintes características: • CVSSv3 Impact Score; • Idade da Vulnerabilidade; • Se existe ameaça ou exploit que explore a vulnerabilidade; • Número de produtos afetados pela vulnerabilidade.
15	Ser capaz de aplicar algoritmos de aprendizagem de máquina para analisar as características relacionadas a vulnerabilidades.
16	Ser capaz de fazer a correlação em tempo real de ameaças ativas contra vulnerabilidades encontradas, incluindo *feeds* de inteligência de ameaças ao vivo.
17	Possuir interfaces de programação de aplicações (API) para automação de processos e integração com: • Aplicações terceiras, possibilitando, no mínimo, a extração de dados para carga em sistemas de Gerenciamento e Correlação de Eventos de Segurança (SIEM); e • aplicações de Gerenciamento de Serviços de TI (ITSM) para as vulnerabilidades encontradas, permitindo o agrupamento no chamado por ações corretivas.
18	Permitir a instalação de agentes em estações de trabalho e servidores, para varredura diretamente no sistema operacional.
19	Possuir conectores para, pelo menos, as seguintes plataformas: • Amazon Web Service (AWS); • Microsoft Azure; • Google Clound Platform.
20	Ser capaz de produzir relatórios nos seguintes formatos: PDF, CSV, HTML e em formato de texto, o qual po-

4.1.2. Requisitos Tecnológicos (Res. CNJ nº 182/2013, art. 4º)	
ID	**Requisito**
	derá ser DOCX, ODT ou RTF.
21	Possuir recurso de monitoria passiva do tráfego de rede para identificação de anomalias, novos dispositivos e desvios de padrões observados.
22	Ser licenciada para o uso ilimitado de sensores passivos de rede para realizar o monitoramento em tempo real. Os sensores devem possuir, no mínimo, as seguintes funcionalidades: • Execução de verificação completa do sistema (rede), adequada para qualquer *host*; • Verificação sem recomendações da rede, para que se possa personalizar totalmente as configurações da verificação; • Autenticação de *hosts* e enumeração de atualizações ausentes; • Execução de varredura simples para descobrir *hosts* ativos e portas abertas; • Utilização de um *scanner* para verificar aplicativos da web; • Avaliação de dispositivos móveis; • Auditoria de configuração de serviços em nuvem de terceiros; • Auditoria de configuração dos gerenciadores de dispositivos móveis; • Auditoria de configuração dos dispositivos de rede; • Auditoria de configurações do sistema em relação a uma linha de base conhecida; • Detecção de desvio de segurança Intel AMT; • Verificação de *malware* nos sistemas Windows e Unix.
23	Permitir determinar, em tempo real, quais portas de serviços (UDP/TCP) estão abertas em determinado ativo.
24	Ser capaz de realizar em tempo real a descoberta de novos ativos para, no mínimo: • serviços de bancos de dados; • hipervisores (pelo menos VMWare ESX/ESXi); • dispositivos móveis; • dispositivos de rede; • *endpoints*; • aplicações.
25	Ser capaz de em tempo real detectar logins e downloads de arquivos em um compartilhamento de rede.
26	Permitir identificar vulnerabilidades associadas a servidores SQL no tráfego de rede.
27	Possuir interface para integração com as principais soluções de SIEM de mercado, tais como IBM QRadar, Microfocus ArcSight e Splunk.
28	Possibilitar a realização de cópias de segurança, funcionamento em alta disponibilidade e criptografia de todos os dados armazenados.
29	A atualização das ameaças deve ocorrer diariamente e sem interrupção dos serviços.
30	Configuração de segurança e acesso à gerência da solução: • Os dados armazenados nos servidores da solução devem ser criptografados, ao menos, com o algo-

4.1.2. Requisitos Tecnológicos (Res. CNJ nº 182/2013, art. 4º)	
ID	**Requisito**
	ritmo AES-256 bits e possuir *logs* de acesso; • Os dados em trânsito devem usar ao menos o algoritmo TLS 1.2 de chave 2048 bits; • Os dados em trânsito devem ser criptografados ao menos com o algoritmo AES-128 bits; • Os algoritmos de *hash* devem usar ao menos o algoritmo SHA-256; • Será aceito como comprovação critérios de criptografia, publicação em site do fabricante ou declaração do próprio fabricante; • Somente servidores da CONTRATANTE ou pessoa por ela autorizada poderão ter acesso aos dados da solução; • A solução deve permitir a criação de, no mínimo, 20 contas para gerência e acesso aos relatórios, sem custo adicional; • A empresa contratada não poderá ter acesso à rede interna da CONTRATANTE e todo o tráfego de dados deverá ser de saída e iniciado pelos *scanners* (*on-premise*).
31	**Dos Relatórios.** A solução deve: 1. Ser capaz de executar relatórios periódicos de acordo com a frequência estabelecida pelo administrador, bem como a geração de relatórios sob demanda; 2. Possibilitar a criação de relatórios baseados na seleção de ativos, permitindo inclusive a seleção de todos os ativos existentes; 3. Suportar a criação de relatórios criptografados (protegidos por senha configurável); 4. Suportar o envio automático de relatórios para destinatários específicos; 5. Permitir definir a frequência na geração dos relatórios para, ao menos: diário, mensal, semanal e anual; 6. Permitir especificar níveis de permissão nos relatórios para usuários e grupos específicos; 7. Fornecer relatórios do tipo *"scorecard"* para as partes interessadas da empresa; 8. Fornecer relatórios de correções aplicadas, classificados pelos seguintes critérios: grupo de ativos, usuários e vulnerabilidades. 9. Possuir ou permitir a criação de relatórios com as seguintes informações: ◦ *Hosts* verificados sem credenciais; ◦ As 100 vulnerabilidades mais críticas (top 100); ◦ Os 10 *hosts* mais infectados por malwares (top 10); ◦ *Hosts* exploráveis por *malwares*; ◦ Total de vulnerabilidades que podem ser exploradas pelo *metasploit*; ◦ Vulnerabilidades críticas e exploráveis; ◦ Máquinas com vulnerabilidades que podem ser exploradas.
32	Permitir mecanismo de varredura baseado em inferência com técnicas de varredura não intrusivas.
33	Possuir *dashboards* customizáveis onde o administrador pode criar, editar ou remover painéis ou *widgets* de acordo com a necessidade.
34	Ser capaz de inventariar todos os ativos da rede local e publicados na Internet, sem limites de endereços IPs.

4.1.2. Requisitos Tecnológicos (Res. CNJ nº 182/2013, art. 4º)	
ID	**Requisito**
35	Ser capaz de realizar varreduras (*scans*) de vulnerabilidades para, no mínimo, 350 (trezentos e cinquenta) IPs.
36	Ser licenciada para um número ilimitado de *scanners* (prevendo redundância).
37	Ser capaz de medir e reportar ameaças.
38	Ser capaz de visualizar ameaças críticas ao ambiente monitorado.
39	Realizar varreduras em uma variedade de sistemas operacionais, suportando, pelo menos, *hosts* baseados em Windows, Linux e Mac OS, assim como *appliances* virtuais.
40	Suportar vários mecanismos de varredura distribuídos em diferentes localidades e regiões e gerenciar todos por uma console central.
41	**Agentes de software.** A solução deve fornecer agentes instaláveis em sistemas operacionais, pelo menos, Windows, Linux e Mac OS, para o monitoramento contínuo de configurações e vulnerabilidades. • A solução deve permitir o monitoramento para varredura diretamente no sistema operacional, tanto através dos agentes quanto sem a necessidade dos agentes.
42	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. • 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.
43	Ser configurável para permitir a otimização das parametrizações de varredura.
44	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.
45	Fornecer a capacidade de escalar privilégios nos destinos, do acesso de usuário padrão até acesso de sistema ou administrativo.
46	Ser capaz de realizar pesquisas de dados confidenciais.
47	**Gerência de vulnerabilidades em aplicações e sítios web**. Possuir módulo para realizar varreduras de vulnerabilidades para, no mínimo, 20 aplicações Web, atendendo ao seguinte: 1. Deve cobrir, no mínimo, mas não se limitando a base de ameaças apontadas pelo OWASP Top 10, CWE e WASC; 2. Executar varreduras em sistemas Web através de seus endereços IP ou FQDN (DNS); 3. Identificar vulnerabilidades de divulgação de dados, como vazamento de informações de identificação pessoal; 4. 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. Permitir a execução da função *crawler*, que consiste na navegação para descoberta das URLs existentes na aplicação;

4.1.2. Requisitos Tecnológicos (Res. CNJ nº 182/2013, art. 4º)	
ID	**Requisito**
	6. Suportar a integração com o softwares de automação de testes para permitir sequências de autenticação complexas; 7. Realizar testes/varreduras em aplicações separadas simultaneamente, limitadas ao número de licenças; 8. Suporte a ferramentas para construção de requisições e análise de respostas de aplicações WEB, API's e *web services*, tais como *Postman Collections*; 9. Oferecer suporte à capacidade de testar novamente a vulnerabilidade específica que foi detectada anteriormente no aplicativo web; 10. Ser capaz de utilizar *scripts* customizados de *crawling* com parâmetros definidos pelo usuário; 11. Ser capaz de excluir determinadas URLs da varredura através de expressões regulares; 12. Ser capaz de excluir determinados tipos de arquivos através de suas extensões; 13. 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; 13.2. Número máximo de requisições HTTP(S) por segundo; 14. Ser capaz de agendar a varredura e determinar sua frequência entre uma única vez, diária, semanal, mensal e anual; 15. Suportar o envio de notificações por email; 16. Ser compatível com avaliação de web services REST e SOAP; 17. Suportar os seguintes esquemas de autenticação: a) Autenticação Básica (*digest*); b) NTLM; c) Autenticação de *cookies*; 18. Ser capaz de importar *scripts* de autenticação previamente configurados pelo usuário; 19. Ser capaz de exibir os resultados das varreduras de forma temporal para acompanhamento de correções e introdução de novas vulnerabilidades; 19.1. Os resultados devem ser apresentados agregados por vulnerabilidades ou por aplicações; 19.2. Para cada vulnerabilidade encontrada, deve ser exibido detalhes e evidências; 19.3. Cada vulnerabilidade encontrada deve conter também soluções propostas para mitigação ou remediação; ***20. Serviço de Detecção de Malware.*** A solução de análise deve: 20.1. Utilizar a plataforma de gerenciamento de vulnerabilidades existente; 20.2. Permitir visualizar o acompanhamento das atividades de verificação, páginas infectadas e tendências de infecção por *malware*; 20.3. Fornecer relatórios de resumo geral de todas as aplicações web e resumo de uma aplicação

4.1.2. Requisitos Tecnológicos (Res. CNJ nº 182/2013, art. 4º)

ID	Requisito
	específica, que serão exportados para os formatos XML, HTML ou PDF. 20.4. 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; x) Redmine.

4.1.3. Requisitos Não-funcionais (Res. CNJ nº 182/2013, art. 3º)

ID	Tipo	Requisito
1	Contratual/ Licenciamento	O licenciamento da solução deve incluir todas as funcionalidades. Todas as licenças de uso de software devem ser registradas, na data da entrega, em nome da Contratante no site do fabricante.
2	Contratual/Garantia	A contratação é composta do fornecimento de licenciamento de software com garantia e suporte técnico pelo período de 60 (sessenta) meses.
3	Contratual	Todas as atividades envolvidas serão acompanhadas e coordenadas por equipe

		técnica da COINT/SESRE, do TRE-CE.
4	Qualidade	A CONTRATADA deverá interagir com a equipe técnica do TRE-CE para dirimir dúvidas/questionamentos relacionadas aos serviços prestados.

4.2. Análise das Soluções Disponíveis no Mercado de TIC (Art. 14, I, a)

4.2.1. Alternativas no Mercado de TIC (Art. 14, II, c, 2)

Dentre as soluções existentes no mercado com licenciamento comercial aderentes aos requisitos apresentados na Tabela 1, identificam-se duas abordagens distintas:

1. **Soluções com gerenciamento e armazenamento em nuvem.** Neste tipo, os dados críticos da gestão de vulnerabilidades da rede institucional é mantida em base sob a guarda da fabricante contratada, acessível pela CONTRATANTE pela internet.
2. **Soluções com gerenciamento e armazenamento próprio (*on premisse*)**. Neste tipo de solução, os dados críticos da gestão de vulnerabilidades da rede institucional fica sob a responsabilidade direta da CONTRATANTE, que deve cuidar de sua guarda.

A pesquisa e análise dos produtos comerciais foi feita de modo colaborativo entre diversos TREs. A Tabela 2 indica os produtos levantados, bem como seu custo estimado, conforme propostas de referência, enviadas ao grupo colaborativo.

Tabela 2: Produtos comerciais de gestão de vulnerabilidades

Soluções de gestão de vulnerabilidades com licença comercial			
Seq.	**Produto**	**Fabricante**	**Categoria**
1	Tenable.io Vulnerability Management e Tenable.io Web Application Scanning	Tenable - https://tenable.com	On Cloud e On Premisse
2	Qualys VM e Qualys WAS	Qualys	On Cloud
3	IVM – InsightVM e IAS – InsightAppSec	Rapid7	On Cloud e On Premisse

4.2.2. Software livre ou Software Público (Art. 14, II, c)

Em software aberto, existe a alternativa de se adotarem diferentes soluções de software livre e integrá-las para "montagem" da solução, a saber: OpenVAS[4] e Nmap[5].

4.2.3. Modelo Nacional de Interoperabilidade – MNI (Art. 14, II, d)

Segundo o CNJ, o Modelo Nacional de Interoperabilidade visa *"estabelecer os padrões para intercâmbio de informações de processos judiciais e assemelhados entre os diversos órgãos de administração de justiça, e além de servir de base para implementação das funcionalidades pertinentes no âmbito do sistema processual"*[6]. Os requisitos da solução já estabelecem critérios de interoperabilidade por meio de arquivos de dados em formatos padrão de mercado (CSV, etc.), bem como a exigência de suporte a interface de programação de aplicações (API), o que favorece a interoperabilidade da solução com outros sistemas e soluções de TIC.

4.2.4. Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil (Art. 14, II, e)

"ICP, ou Infra-estrutura de Chaves Públicas, é a sigla no Brasil para PKI - Public Key Infrastructure -, um conjunto de técnicas, práticas e procedimentos elaborado para suportar um sistema criptográfico com base em certificados digitais."[7]. É prerrogativa do Comitê Gestor da ICP-Brasil[8] estabelecer as políticas e normas relacionadas ao tema. Os requisitos da solução já estabelecem exigências mínimas de criptografia que utilizam algoritmos e modelos padrão de mercado.

4.2.5. Modelo de Requisitos Moreq-Jus (Art. 14, II, f)

"O Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Poder Judiciário (Moreq-Jus) apresenta os requisitos que os documentos digitais produzidos pelo Judiciário e os sistemas informatizados de gestão documental deverão cumprir, no intuito de garantir a segurança e a preservação das informações, assim como a comunicação com outros sistemas"[9]. Desta forma, este modelo trata de especificações para aplicações e sistemas corporativos em si e, portanto, não se aplica à presente demanda.

4 https://www.openvas.org/

5 https://nmap.org/

6 http://www.cnj.jus.br/tecnologia-da-informacao/comite-nacional-da-tecnologia-da-informacao-e-comunicacao-do-poder-judiciario/modelo-nacional-de-interoperabilidade

7 http://icp-brasil.certisign.com.br/

8 http://www.iti.gov.br/icp-brasil/comite-gestor

9 http://www.cnj.jus.br/programas-e-acoes/pj-proname/sistema-moreq-jus

4.2.6. Contratações Públicas Similares (Art. 14, I, b)

Como já explicitado, os presentes estudos foram realizados em colaboração com outros TREs ao longo deste ano. A contratação de referência para este presente estudo é a Intenção de Registro de Preços (IRP) nº 22/2020 do TRE/PB (UASG: 70 009)[10], na qual se sugere a participação deste TRE/CE antes da realização do certame (partícipe). A referida IRP é relacionada juntamente a aquisições anteriores, de TREs, na Tabela 3, adiante.

Tabela 3: Aquisições públicas de soluções de gerenciamento de vulnerabilidades. Fonte: Comprasnet.

UASG Gerenciadora	Licitação	Data
Tribunal Regional Eleitoral do Paraná	03/2020 / Doc. Nº 195 547/2020	06/03/20
Tribunal Regional Eleitoral da Paraíba	**IRP 22/2020 / Doc. Nº 195 373/2020**	**12/11/2020**

Detalhamentos de qualquer uma das aquisições podem ser obtidos diretamente no sistema Comprasnet, na página de busca de Pregão[11], pela identificação a UASG gerenciadora e da licitação.

Salienta-se que cada órgão possui necessidades específicas e, em relação às aquisições elencadas, os equipamentos nelas adquiridos podem conter especificações inferiores ou superiores aos requeridos na presente demanda do TRE/CE.

- Outras Soluções Disponíveis (Art. 14, II, a)

Além das soluções comerciais ou integração de soluções de código aberto, alternativas já explicadas, não se vislumbram soluções alternativas à presente demanda.

4.3. Escolha e Justificativa da Solução (Art. 14, IV)

4.3.1. Análise das alternativas disponíveis.

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

10 Intenção de Registro de Preços (IRP) nº 22/2020 do TRE/PB (UASG: 70 009). Documento PAD nº 195 373/2020.

11 http://comprasnet.gov.br/acesso.asp?url=/livre/pregao/ata0.asp

As soluções baseadas em nuvem (*on cloud*) apresentam 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, bem como testes em aplicações Web. Porém como os dados armazenados pela ferramenta (vulnerabilidades dos ativos de TIC) são considerados muito sensíveis, não é recomendável estarem armazenados em nuvem pública.

O armazenamento de dados sensíveis em nuvem é ainda desaconselhado pela Norma Complementar 14[12] do Gabinete de Segurança Institucional da Presidência da República:

> "5.2.2 Informação sigilosa: como regra geral, deve ser evitado o tratamento em ambiente de computação em nuvem, conforme disposições a seguir:
>
> 5.2.2.1. Informação classificada: é vedado o tratamento em ambiente de computação em nuvem;
>
> 5.2.2.2. Conhecimento e informação contida em material de acesso restrito: é vedado o tratamento em ambiente de computação em nuvem;
>
> (…)
>
> 5.3 Deve ser assegurado que dados, metadados, informações e conhecimento, produzidos ou custodiados por órgão ou entidade da APF, bem como suas cópias de segurança, residam em território brasileiro;"

As soluções baseadas em gerenciamento em rede local do tribunal (*on premisse*) apresentam um valor de aquisição adequado e menor do que as soluções *on cloud*. Apesar das soluções do tipo *on premisse* trazerem 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 TRE, e não em nuvem pública. Todas os requisitos de funcionalidades do projeto também são atendidos por esse cenário. As soluções analisadas Tenable (Tenable.io) 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 às soluções *on premisse* é o fato de que, após o término do suporte, a STIC continuará a ter acesso à ferramenta, ainda que sem o direito de recebimento de atualizações de versão e de novas vulnerabilidades.

12 Norma Complementar 141 do Gabinete de Segurança Institucional da Presidência da República. Documento PAD nº 195 442/2020. Em: https://repositorio.cgu.gov.br/handle/1/42 764. Acesso em 09/11/2020.

Sendo assim, opta-se pela alternativa de contratação de solução comercial baseada no gerenciamento em rede local do tribunal, tendo em vista o menor custo teórico e o fato de operar sem armazenar em nuvem pública os dados sensíveis, que são as vulnerabilidades dos ativos de TIC do Tribunal.

4.3.2. Descrição da Solução (Art. 14, IV, a)

Objeto: Aquisição de licenciamento de software de gestão integrada de vulnerabilidades e análise dinâmica de aplicações web baseada em gerenciamento e armazenamento na rede local do tribunal, com modelo de subscrição por 60 (sessenta) meses ou de licença perpétua com suporte de 60 (sessenta) meses. A composição do objeto é definida na Tabela 4 e suas especificações técnicas serão detalhadas no Termo de Referência.

Tabela 4: Descrição e quantitativos previstos nesta contratação, por item.

Item	Descrição	Demanda	Valor estimado
1.	Licenciamento de plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos de rede, gerenciada localmente (*on premisse*), para, no mínimo, 350 (trezentos e cinquenta) IPs, pelo período de 60 (sessenta) meses.	1	R$ 360.894,75
2.	Licenciamento para solução de análise dinâmica em aplicações Web, gerenciada localmente (*on premisse*), para, no mínimo, 15 (quinze) domínios (FQDN), pelo período de 60 (sessenta) meses.	1	R$ 111.977,00
3.	Instalação e configuração da solução.	1	R$ 9.106,00
4.	Repasse tecnológico *"hands-on"* em formato de treinamento, com duração mínima de 20h, para 8 pessoas.	1	R$ 6.421,00
	VALOR TOTAL ESTIMADO:		**R$ 488.398,75**

4.4. Orçamento Estimado (Art. 14, II, g)

Como parte do trabalho colaborativo entre TREs e TSE, do qual este estudo é produto resultante, foram realizadas cotações de preços de referência ao mercado, estando as propostas recebidas incluídas nos autos como documento nº 195 761/2020. Os valores obtidos nas propostas para a demanda do TRE/CE são apresentados na planilha constante no documento nº 195 776/2020.

4.5. Análise dos Custos Totais da Demanda (Art. 14, III)

Os custos estimados da demanda são, conforme a planilha de cotações, documento nº 195 776/2020, apresentados resumidos na própria Tabela 4.

4.6. Alinhamento da Solução (Art. 14, IV, b)

A presente aquisição está alinhada com o Planejamento Estratégico Institucional (PEI) e o de Tecnologia da Informação e Comunicação (PETIC) do TRE/CE, vindo a atender aos objetivos estratégicos apontados na seção 3.1.1 – Objetivos Estratégicos (Res. CNJ 182/2013, Art.12, § 5º, I).

A presente contratação **está prevista** no Plano de Aquisições de TIC para 2021, constituindo-se fundamental para aumentar a segurança da informação da infraestrutura do TRE/CE.

4.6.1. Benefícios Esperados (Art. 14, IV, c)

a) Maior garantia de disponibilidade dos serviços de TIC da nova sede do TRE/CE;
b) Gerenciamento eficaz das vulnerabilidades cibernéticas do ambiente operacional de tecnologia da informação do TRE/CE;
c) Mitigação do risco de ataques cibernéticos bem-sucedidos, que comprometeriam os dados e serviços de TIC do TRE/CE, tal como o evento ocorrido com o STJ.

4.6.2. Relação Demanda Prevista / Quantidade CONTRATADA (Art. 14, IV, d)

A relação encontra-se prevista na Tabela 4, e foi avaliada com base na quantidade atual de servidores físicos e virtuais operando no *data center* do TRE/CE.

4.6.3. Adequação do Ambiente (Art. 14, V, a, b, c, d, e, f)

Infraestrutura de rede

A solução deverá rodar no data center do TRE/CE, já disponível.

Impacto ambiental

Por ser uma solução de software, esta opção não se aplica.

5. Sustentabilidade da Solução

A CONTRATADA deverá adotar as seguintes práticas de sustentabilidade na execução dos serviços, quando couber:

- Que os bens sejam constituídos, no todo ou em parte, por material reciclado, atóxico, biodegradável, conforme normas ABNT NB-R 15 448-1 e 15 448-2;
- Que sejam observados os requisitos ambientais para a obtenção de certificação do Instituto Nacional de Metrologia, Normalização e Qualidade Industrial – INMETRO como produtos sustentáveis ou de menor impacto ambiental em relação aos seus similares;

- Que os bens devam ser preferencialmente, acondicionados em embalagem individual adequada, com o menor volume possível, que utilize materiais recicláveis, de forma a garantir a máxima proteção durante o transporte e o armazenamento;
- Que os bens não contenham substâncias perigosas em concentração acima da recomendada na diretiva *ROHS (Restriction of Certain Hazardous Substances)*, tais como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr(VI)), cádmio (Cd), bifenil-polibromados (PBBs), éteres difenil-polibromados (PBDES);
- Que sejam utilizados produtos de limpeza e conservação de superfícies e objetos inanimados que obedeçam às classificações e especificações determinadas pela ANVISA;
- Respeite as Normas Brasileiras (NBR) publicadas pela Associação Brasileira de Normas Técnicas sobre resíduos sólidos; e preveja a destinação ambiental adequada das pilhas e baterias usadas ou inservíveis, segundo disposto na Resolução CONAMA nº 257, de 30 de junho de 1999.

6. Sustentação do Contrato (Res. CNJ 182/2013, Art. 15)

6.1. Recursos Materiais e Humanos (Art. 15, I)

A gestão do contrato estão indicados na seção 7.7 – Equipe de Gestão da Contratação (Art. 16, VIII). A equipe da SESIC realizará, sob coordenação da COINT, os testes necessários no software contratado, para que se dê o aceite definitivo à contratação.

6.2. Descontinuidade do Fornecimento (Art. 15, II)

Encerramento repentino do contrato – Ações de contingência e respectivos responsáveis

1. Realizar o planejamento de uma nova contratação em suprimento a necessidade gerada pelo encerramento do contrato. (STI/COINT).

Atraso à prestação dos serviços – Ações de contingência e respectivos responsáveis

- Aplicação de sanções previstas em contrato e reunião com o representante para alinhamento das cláusulas contratuais. (SAD/COLIC e STI/COINT).
- Verificar a viabilidade da continuidade do contrato (STI/COINT).

6.3. Transição Contratual (Art. 15, III, a, b, c, d, e)

O TRE/CE não dispõe atualmente de solução similar para a presente demanda, não havendo, portanto, o que se falar em termos de transição contratual.

6.4. Estratégia de Independência Tecnológica (Art. 15, IV, a, b)

A solução prevê o serviço de instalação e configuração do *software* incluindo o repasse tecnológico, pela empresa CONTRATADA, à equipe técnica do TRE/CE, de forma a promover sua independência do fornecedor. Adicionalmente, deve-se prever possibilidade de contratação adicional futura para capacitação na tecnologia a ser adquirida.

7. Estratégia para a Contratação (Res. CNJ 182/2013, Art. 16.)

7.1. Natureza do Objeto (Art. 16, I)

Esse projeto tem por objetivo o licenciamento de *softwares* de gestão de vulnerabilidades cibernéticas, caracterizando-se como objeto de natureza comum. As especificações técnicas da presente solução serão detalhadas no Termo de Referência.

7.2. Parcelamento e Adjudicação do Objeto (Art. 16, II e III)

O objeto da presente aquisição deverá ser adquirido integralmente em uma única contratação, com adjudicação do lote integral.

7.3. Modalidade e Tipo de Licitação (Art. 16, IV)

Sugere-se a participação na Intenção de Registro de Preços (IRP) nº 22/2020 do TRE/PB (UASG: 70 009)[10.]

7.4. Classificação e Indicação Orçamentária (Art. 16, V)

A classificação orçamentária será indicada pela Secretaria de Orçamento e Finanças (SOF).

7.5. Vigência da Prestação de Serviço (Art. 16, VI)

Vigência do contato por 12 (doze) meses a partir da publicação de seu extrato no DOU.

Vigência do licenciamento e garantia do fabricante pelo período de 60 (sessenta) meses.

7.6. Equipe de Apoio à Contratação (Art. 16, VII)

Para prestar apoio à Comissão Permanente de Licitação em suas dúvidas, respostas aos questionamentos, recurso e impugnações, bem como na análise e julgamento das propostas das licitantes, indicam-se os seguintes servidores:

Coordenadoria de Infraestrutura Tecnológica – COINT

Jonas de Araújo Luz Jr.
E-mail: jonas@tre-ce.jus.br

Lauro Salmito Pinheiro
E-mail: lauro@tre-ce.jus.br

Seção de Suporte Operacional e Segurança da Informação (SESIC)

Ticiano do Nascimento Diniz
E-mail: ticiano@tre-ce.jus.br

7.7. Equipe de Gestão da Contratação (Art. 16, VIII)

7.7.1. Gestão dos contratos

- Titular: Chefe da Seção de Suporte Operacional e Segurança da Informação (SESIC)
- Suplente: Coordenador de Infraestrutura Tecnológica (COINT).

8. Análise de Riscos (Res. CNJ 182/2013, Art. 17.)

8.1. Identificação e Outros Requisitos Associados aos Riscos (art. 17, I, II, III, IV e V)

A matriz de riscos da presente contratação é apresentada na seção 8.2 – MATRIZ DE RISCOS E CONTROLES (Resolução nº 563/2014), em anexo.

8.2. MATRIZ DE RISCOS E CONTROLES (*Resolução nº 563/2014*)

Seq.	RISCOS					ATIVIDADES DE CONTROLE(*)			
	Descrição	P	I	N	Responsável	Descrição	Responsável	Status	Prazo
1	Não envolvimento de qualquer representante da EPC no processo de Estudos Preliminares / Termo de Referência.	4	1	4	DIGER	Monitorar e garantir a participação de todos os representantes.	DIGER	CN	-
2	Contratação fracassar no exercício financeiro.	3	5	15	COINT e COLIC	Monitoramento de prazos do processo de contratação.	SAD/COLIC	**CA**	-
3	Atraso na entrega das licenças no exercício financeiro.	3	4	12	COINT	Fiscalização da execução contratual.	STI/COINT	**CI**	-
4	Incorreções, ausências, falhas e defeitos no licenciamento fornecidos.	1	5	5	COINT	Fiscalização da execução contratual.	STI/COINT	**CI**	-
5	Atraso no fornecimento dos licenciamentos.	2	3	6	COINT	Fiscalização da execução contratual.	STI/COINT	**CI**	-
6	Crescimento da demanda superior ao estimado.	1	3	3	COINT	Acompanhamento da demanda frente a contratação.	STI/COINT	**CA**	**Dez. 2021**
Elaborado por: Jonas de Araújo Luz Jr.									
Revisado por: Carlos Antônio Sampaio de Melo									

P – Probabilidade: 1(muito baixa) / **2**(baixa) / **3**(média) / **4**(alta) / **5**(muito alta)
I – Impacto: 1(muito baixo) / **2**(baixo) / **3**(médio) / **4**(alto) / **5**(muito alto)
N – Nível de Risco (P x I)**: 1-4**(baixo) / **5-11**(médio) / **12-19**(alto) / **20-25**(extremo)
Status da atividade de controle: **CN** (controle não implantado) / **CI** (controle implantado) / **CA** (controle a aprimorar)
(*) Atividade de controle a ser implantada ou a ser aperfeiçoada no exercício seguinte deverá ser registrada no SIPOG, no rol de atividades sem demanda orçamentária do Pla - nejamento Setorial.

ESTUDOS PRELIMINARES

I – ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO

1 ESPECIFICAÇÃO DOS REQUISITOS

1.1 DE NEGÓCIO

1.1.1 A solução deverá:

1.1.1.1 Permitir a gestão de vulnerabilidades em sistemas operacionais.

1.1.1.1.1 Testar os *hosts* (físicos e virtuais), comparando as bases de dados de vulnerabilidades mantidas por organizações especializadas em segurança da informação e por grandes fabricantes de *software*.

1.1.1.2 Permitir a gestão de vulnerabilidades em sistemas e páginas *web*.

1.1.1.2.1 Testar as aplicações e páginas *web*, internas e externas, comparando as bases de dados de vulnerabilidades mantidas por organizações especializadas em segurança da informação e por grandes fabricantes de *software*.

1.1.1.3 Ser capaz de emissão de relatórios dos testes realizados, das vulnerabilidades encontradas e de sua correção, necessários ao acompanhamento das atividades de identificação, análise, priorização e mitigação de riscos.

1.1.2 Atualmente existe a necessidade de aquisição de ferramenta de gestão de vulnerabilidades, conforme abaixo:

Item	Descrição	Tipo
1	Licenciamento de plataforma de gestão de vulnerabilidades e auditoria de configurações	Ativos de rede
2	Licenciamento para solução de análise dinâmica	Aplicações *Web*
3	Serviço de instalação e configuração da solução	-
4	Repasse tecnológico	Por um período mínimo de 20 (vinte) horas
5	Suporte técnico	04 (quatro) horas de serviço especializado

Documento assinado digitalmente por:		
FRANCISCO DE A. PAIVA LEAL:92440776 23/10/2020 18:57:47	DENILSON BASTOS DA SILVA:20024241 23/10/2020 19:21:28	Marat Soares Teixeira 23/10/2020 19:41:40

Documento assinado digitalmente por:
Marcos Flavio Nascimento Maia 31/10/2020 10:06:58

1.2 DE CAPACITAÇÃO

1.2.1 Haverá necessidade de treinamento ou repasse tecnológico, presencial ou a distância, no mínimo de **20 (vinte) horas**, visando capacitar os servidores da Secretaria de Tecnologia da Informação e Eleições (STIE) no uso da ferramenta.

1.3 LEGAIS

1.3.1 A contratação obedecerá às regras gerais de fornecimento ao Poder Público, inexistindo requisitos legais específicos para essa contratação.

1.4 MANUTENÇÃO

1.4.1 Suporte técnico deve estar disponível durante a vigência de uso da licença.

1.4.2 Atualizações da solução disponível durante a vigência de uso da licença.

1.5 TEMPORAIS

1.5.1 A fornecedora da solução terá até **05 (cinco) dias** contados após a formalização da contratação para fornecer os *softwares* ou as subscrições contratadas.

1.6 DE SEGURANÇA

1.6.1 A fornecedora da solução deverá obedecer aos critérios, padrões, normas e procedimentos operacionais adotados pela JUSTIÇA ELEITORAL, em especial:

1.6.1.1 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.

1.6.1.2 Da gestão de ativos.

1.6.1.3 Manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de interesse da JUSTIÇA ELEITORAL ou de terceiros de que tomar conhecimento em razão da execução do objeto desta contratação devendo orientar seus funcionários nesse sentido.

1.6.1.4 Submeter seus recursos técnicos aos regulamentos de segurança e disciplina instituídos pela JUSTIÇA ELEITORAL, durante o tempo de permanência nas suas dependências, observando a Portaria 226/2018-GP-TRE/RN, que dispõe sobre as medidas de controle de acesso, circulação e permanência de pessoas nos prédios do Edifício-Sede do TRE/RN, do Centro de Operações da Justiça Eleitoral (COJE), Fórum Eleitoral de Natal e, no que couber, aos prédios das Zonas Eleitorais do Interior do Estado.

Documento assinado digitalmente por:		
FRANCISCO DE A. PAIVA LEAL:92440776 23/10/2020 18:57:47	DENILSON BASTOS DA SILVA:20024241 23/10/2020 19:21:28	Marat Soares Teixeira 23/10/2020 19:41:40

Documento assinado digitalmente por:
Marcos Flavio Nascimento Maia 31/10/2020 10:06:58

1.7 SOCIAIS, AMBIENTAIS E CULTURAIS

1.7.1 É de responsabilidade da empresa fornecedora da solução 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.

1.7.2 O TRE/RN 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.

1.7.3 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.

1.8 DE ARQUITETURA TECNOLÓGICA

1.8.1 Tendo como base os requisitos funcionais definidos, foram identificados os seguintes requisitos tecnológicos:

1.8.1.1 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 (duzentos e cinquenta) *IPs*.

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

1.8.1.3 A solução de gestão de vulnerabilidades deve suportar varreduras de dispositivos de *IoT*.

1.8.1.4 A solução deve ser capaz de identificar no mínimo 50.000 (cinquenta mil) *CVEs (Common Vulnerabilities and Exposures).*

1.8.1.5 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.

1.8.1.6 A solução deve atribuir a todas as vulnerabilidades uma severidade baseada no *CVSSv3 score*.

1.8.1.7 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.

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

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

Documento assinado digitalmente por:		
FRANCISCO DE A. PAIVA LEAL:92440776 23/10/2020 18:57:47	DENILSON BASTOS DA SILVA:20024241 23/10/2020 19:21:28	Marat Soares Teixeira 23/10/2020 19:41:40

Documento assinado digitalmente por:
Marcos Flavio Nascimento Maia 31/10/2020 10:06:58

1.8.1.10 A solução deve possuir um sistema de busca de informações de um determinado ativo com, no mínimo, as seguintes características:

1.8.1.10.1	Por sistema operacional
1.8.1.10.2	Por um determinado software instalado
1.8.1.10.3	Por ativos impactados por uma determinada vulnerabilidade

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

1.8.1.12 A solução deve permitir aceitar o risco de uma determinada vulnerabilidade encontrada no ambiente.

1.8.1.13 A solução deve possibilitar alterar a criticidade de determinada vulnerabilidade de forma manual.

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

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

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

1.8.1.16.1	*CVSSv3 Impact Score*
1.8.1.16.2	Idade da Vulnerabilidade
1.8.1.16.3	Se existe ameaça ou *exploit* que explore a vulnerabilidade
1.8.1.16.4	Número de produtos afetados pela vulnerabilidade

1.8.1.17 A solução deve ser capaz de fazer a correlação em tempo real de ameaças ativas contra vulnerabilidades encontradas, incluindo *feeds* de inteligência de ameaças ao vivo.

1.8.1.18 A solução deve possuir uma *API* para automação de processos e integração com aplicações terceiras permitindo, no mínimo, a extração de dados para carga no *SIEM*.

1.8.1.19 A solução 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.

1.8.1.20 A solução deve permitir a instalação de agentes em estações de trabalho e servidores, para varredura diretamente no sistema operacional.

1.8.1.21 Se for baseada em nuvem, a solução deve possuir conectores para, no mínimo, as seguintes plataformas:

1.8.1.21.1	*Amazon Web Service (AWS)*
1.8.1.21.2	*Microsoft Azure*
1.8.1.21.3	*Google Cloud Platform*

Documento assinado digitalmente por:		
FRANCISCO DE A. PAIVA LEAL:92440776 23/10/2020 18:57:47	DENILSON BASTOS DA SILVA:20024241 23/10/2020 19:21:28	Marat Soares Teixeira 23/10/2020 19:41:40

Documento assinado digitalmente por:
Marcos Flavio Nascimento Maia 31/10/2020 10:06:58

1.8.1.22 A solução deve ser capaz de produzir relatórios nos seguintes formatos: *PDF, CSV* ou *HTML*.

1.8.1.23 A solução deve possuir recurso de monitoria passiva do tráfego de rede para identificação de anomalias, novos dispositivos e desvios de padrões observados.

1.8.1.24 A solução deve ser licenciada para o uso ilimitado de sensores passivos de rede para realizar o monitoramento em tempo real.

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

1.8.1.25.1	Execução de verificação completa do sistema (rede), adequada para qualquer *host*
1.8.1.25.2	Verificação sem recomendações da rede, para que se possa personalizar totalmente as configurações da verificação
1.8.1.25.3	Autenticação de *hosts* e enumeração de atualizações ausentes
1.8.1.25.4	Execução de varredura simples para descobrir *hosts* ativos e portas abertas
1.8.1.25.5	Utilização de um *scanner* para verificar aplicativos da web
1.8.1.25.6	Avaliação de dispositivos móveis
1.8.1.25.7	Auditoria de configuração de serviços em nuvem de terceiros
1.8.1.25.8	Auditoria de configuração dos gerenciadores de dispositivos móveis
1.8.1.25.9	Auditoria de configuração dos dispositivos de rede
1.8.1.25.10	Auditoria de configurações do sistema em relação a uma linha de base conhecida
1.8.1.25.11	Detecção de desvio de segurança *Intel AMT*
1.8.1.25.12	Verificação de *malware* nos sistemas *Windows* e *Unix*

1.8.1.26 A solução deve ser possível determinar em tempo real, quais portas de serviços (*UDP/TCP*) estão abertas em determinado ativo.

1.8.1.27 A solução deve ser capaz de realizar em tempo real a descoberta de novos ativos para no mínimo:

1.8.1.27.1	Bancos de dados
1.8.1.27.2	*Hypervisors* (no mínimo VMWare ESX/ESXi)
1.8.1.27.3	Dispositivos móveis
1.8.1.27.4	Dispositivos de rede
1.8.1.27.5	*Endpoints*
1.8.1.27.6	Aplicações

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

1.8.1.29 A solução deve permitir identificar vulnerabilidades associadas a servidores *SQL* no tráfego de rede.

1.8.1.30 A solução deve possuir interface para integração com as principais soluções de *SIEM* de mercado,

Documento assinado digitalmente por:		
FRANCISCO DE A. PAIVA LEAL:92440776 23/10/2020 18:57:47	DENILSON BASTOS DA SILVA:20024241 23/10/2020 19:21:28	Marat Soares Teixeira 23/10/2020 19:41:40

Documento assinado digitalmente por:
Marcos Flavio Nascimento Maia 31/10/2020 10:06:58

tais como *IBM QRadar, Microfocus ArcSight e Splunk.*

1.8.1.31 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.

1.8.1.32 A atualização das ameaças deve ocorrer diariamente e sem interrupção dos serviços.

1.8.1.33 Configuração de segurança e acesso à gerência da solução:

1.8.1.33.1	Todos os dados armazenados nos servidores da solução devem ser criptografados e possuir logs de acesso
1.8.1.33.2	Os dados em trânsito devem usar ao menos o algorítimo *TLS* 1.2 de chave 2048 *bits*
1.8.1.33.3	Os dados em trânsito devem ser criptografados ao menos com o algorítimo *AES*-128 *bits*
1.8.1.33.4	Os algorítimos de *hash* devem usar ao menos o algorítimo *SHA*-256
1.8.1.33.5	Será aceito como comprovação critérios de criptografia publicação em site do fabricante ou declaração do próprio fabricante
1.8.1.33.6	Os dados armazenados devem ser criptografados ao menos com o algorítimo *AES*-256 *bits*
1.8.1.33.7	Somente servidores do TRE/RN ou pessoa por ela autorizada poderão ter acesso aos dados da solução
1.8.1.33.8	A solução deve permitir a criação de, no mínimo, 20 (vinte) contas para gerência e acesso aos relatórios, sem custo adicional
1.8.1.33.9	A empresa fornecedora da solução não deverá ter acesso a rede interna da contratante e todo trafego de dados deverá ser de saída e iniciado pelos *scanners (on-premises*)

1.8.1.34 Todas as licenças de uso de *software* devem ser registradas, na data da entrega, em nome do TRE/RN no site do fabricante.

1.8.1.35 Dos Relatórios:

1.8.1.35.1	Deve ser capaz de executar relatórios periódicos de acordo com a frequência estabelecida pelo administrador, bem como a geração de relatórios sob demanda
1.8.1.35.2	A solução deve possibilitar a criação de relatórios baseados na seleção de ativos, permitindo inclusive a seleção de todos os ativos existentes
1.8.1.35.3	A solução deve suportar a criação de relatórios criptografados (protegidos por senha configurável)
1.8.1.35.4	A solução deve suportar o envio automático de relatórios para destinatários específicos
1.8.1.35.5	A solução deve ser possível definir a frequência na geração dos relatórios para no mínimo: Diário, Mensal, Semanal e Anual
1.8.1.35.6	A solução deve permitir especificar níveis de permissão nos relatórios para usuários e grupos específicos
1.8.1.35.7	A solução deve fornecer relatórios do tipo "*scorecard*" para as partes interessadas da empresa
1.8.1.35.8	A solução deve fornecer relatórios de correções aplicadas, classificados pelos seguintes critérios: grupo de ativos, usuários e vulnerabilidades

Documento assinado digitalmente por:		
FRANCISCO DE A. PAIVA LEAL:92440776 23/10/2020 18:57:47	DENILSON BASTOS DA SILVA:20024241 23/10/2020 19:21:28	Marat Soares Teixeira 23/10/2020 19:41:40

Documento assinado digitalmente por:
Marcos Flavio Nascimento Maia 31/10/2020 10:06:58

1.8.1.36 A solução deve permitir mecanismo de varredura baseado em inferência com técnicas de varredura não intrusivas.

1.8.1.37 A solução deve possuir ou permitir a criação de relatórios com as seguintes informações:

1.8.1.37.1	*Hosts* verificados sem credenciais
1.8.1.37.2	*Top* 100 Vulnerabilidades mais críticas
1.8.1.37.3	*Top* 10 *Hosts* infectados por *Malwares*
1.8.1.37.4	*Hosts* exploráveis por *Malwares*
1.8.1.37.5	Total de vulnerabilidades que podem ser exploradas pelo *Metasploit*
1.8.1.37.6	Vulnerabilidades críticas e exploráveis
1.8.1.37.7	Máquinas com vulnerabilidades que podem ser exploradas

1.8.1.38 A solução deve possuir *dashboards* customizáveis onde o administrador pode criar, editar ou remover painéis de acordo com a necessidade.

1.8.1.39 A solução deve ser capaz de inventariar todos os ativos da rede local e publicados na Internet, sem limites de endereços *IPs*.

1.8.1.40 A plataforma de *software* deve ser capaz de realizar varreduras (*scans*) de vulnerabilidades para no mínimo 250 Ips.

1.8.1.41 A plataforma de *software* deve ser licenciada para um número ilimitado de *scanners* (prevendo redundância).

1.8.1.42 A solução deve permitir a configuração de vários painéis e *widgets*.

1.8.1.43 A solução deve ser capaz de medir e reportar ameaças.

1.8.1.44 A solução deve ser capaz de visualizar ameaças críticas ao ambiente monitorado.

1.8.1.45 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.

1.8.1.46 A plataforma de *software* deve suportar vários mecanismos de varredura distribuídos em diferentes localidades e regiões e gerenciar todos por uma console central.

1.8.1.47 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.

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

1.8.1.49 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.

1.8.1.50 A plataforma de *software* deve incluir a capacidade de programar períodos de tempo e data onde varreduras não podem ser executadas, por exemplo em determinados dias do mês ou

Documento assinado digitalmente por:		
FRANCISCO DE A. PAIVA LEAL:92440776 23/10/2020 18:57:47	DENILSON BASTOS DA SILVA:20024241 23/10/2020 19:21:28	Marat Soares Teixeira 23/10/2020 19:41:40

Documento assinado digitalmente por:
Marcos Flavio Nascimento Maia 31/10/2020 10:06:58

determinados horários do dia.

1.8.1.51 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.

1.8.1.52 A plataforma de software deve ser configurável para permitir a otimização das parametrizações de varredura.

1.8.1.53 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*.

1.8.1.54 A plataforma de *software* deve fornecer a capacidade de escalar privilégios nos destinos, do acesso de usuário padrão até acesso de sistema ou administrativo.

1.8.1.55 A plataforma de *software* deve ser capaz de realizar pesquisas de dados confidenciais.

1.8.1.56 A solução deve possuir módulo para realizar análise dinâmica em aplicações *Web*:

1.8.1.56.1	A solução deve possuir módulo para realizar varreduras de vulnerabilidades para, no mínimo, 05 (cinco) aplicações *Web*, cobrindo no mínimo, mas não limitando-se a base de ameaças apontadas pelo *OWASP Top 10, CWE* e *WASC*
1.8.1.56.2	A solução de análise deve ser capaz de analisar, testar e reportar falhas de segurança em aplicações *Web*
1.8.1.56.3	A solução de análise deverá ser capaz de executar varreduras em sistemas *Web* através de seus endereços *IPs* ou *FQDN* (*DNS*)
1.8.1.56.4	A solução de análise deve ser capaz de identificar vulnerabilidades de divulgação de dados, como vazamento de informações de identificação pessoal
1.8.1.56.5	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*
1.8.1.56.6	A solução deverá também permitir a execução da função *crawler*, que consiste na navegação para descoberta das *URLs* existentes na aplicação
1.8.1.56.7	A solução de análise deve suportar a integração com o softwares de automação de testes para permitir sequências de autenticação complexas
1.8.1.56.8	A solução de análise deve ser capaz de realizar testes/varreduras em aplicações separadas, simultaneamente limitadas ao número de licenças
1.8.1.56.9	A solução de análise deve oferecer suporte à capacidade de testar novamente a vulnerabilidade específica que foi detectada anteriormente no aplicativo *Web*
1.8.1.56.10	A solução deve ser capaz de utilizar scripts customizados de *crawling* com parâmetros definidos pelo usuário
1.8.1.56.11	A solução deve ser capaz de excluir determinadas *URLs* da varredura através de expressões regulares
1.8.1.56.12	A solução deve ser capaz de excluir determinados tipos de arquivos através de suas extensões

Documento assinado digitalmente por:		
FRANCISCO DE A. PAIVA LEAL:92440776 23/10/2020 18:57:47	DENILSON BASTOS DA SILVA:20024241 23/10/2020 19:21:28	Marat Soares Teixeira 23/10/2020 19:41:40

Documento assinado digitalmente por:
Marcos Flavio Nascimento Maia 31/10/2020 10:06:58

1.8.1.56.13	A solução 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
1.8.1.56.14	A solução deve ser capaz de agendar a varredura e determinar sua frequência entre uma única vez, diária, semanal, mensal e anual
1.8.1.56.15	A solução deve suportar o envio de notificações por email
1.8.1.56.16	A solução deverá ser compatível com avaliação de web services *REST* e *SOAP*
1.8.1.56.17	A solução de análise deve suportar os seguintes esquemas de autenticação: Autenticação Básica (*Digest*). *NTLM*. Autenticação de *Cookies*
1.8.1.56.18	A solução deve ser capaz de importar scripts de autenticação previamente configurados pelo usuário
1.8.1.56.19	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
1.8.1.56.20	Os resultados devem ser apresentados agregados por vulnerabilidades ou por aplicações
1.8.1.56.21	Para cada vulnerabilidade encontrada, deve ser exibido detalhes e evidências
1.8.1.56.22	Cada vulnerabilidade encontrada deve conter também soluções propostas para mitigação ou remediação

Documento assinado digitalmente por:		
FRANCISCO DE A. PAIVA LEAL:92440776 23/10/2020 18:57:47	DENILSON BASTOS DA SILVA:20024241 23/10/2020 19:21:28	Marat Soares Teixeira 23/10/2020 19:41:40

Documento assinado digitalmente por:
Marcos Flavio Nascimento Maia 31/10/2020 10:06:58

1.8.1.56.23	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*
1.8.1.56.24	A solução deve ser capaz de realizar varreduras nos seguintes componentes/aplicações: ◦ *WordPress* ◦ *IIS 6.x e IIS 10.x* ◦ *ASP 6* ◦ *NET 2* ◦ *Apache HTTPD 2.2.x e 2.4.x* ◦ *Tomcat 6.x, 7.x, 8.x e superiores* ◦ *Jetty 8 e superiores* ◦ *Nginx* ◦ *PHP 5.3.x, 5.4.x, 5.6.x, 7.0.x e 7.1.x e superiores* ◦ *Java 1.5, 1.6, 1.7 e 1.8 e superiores* ◦ *Jboss 4.x e 7.x e superiores* ◦ *WildFly 8 e 10 e superiores* ◦ *Plone 2.5.x e 5.2.1.41.x e superiores* ◦ *Zope* ◦ *Python 2.4.4 e superiores* ◦ *J2EE* ◦ *Ansible* ◦ *Joomla* ◦ *Moodle* ◦ *Docker Conteiner* ◦ *Elk* ◦ *GIT* ◦ *Grafana* ◦ *Redmine*

Documento assinado digitalmente por:		
FRANCISCO DE A. PAIVA LEAL:92440776 23/10/2020 18:57:47	DENILSON BASTOS DA SILVA:20024241 23/10/2020 19:21:28	Marat Soares Teixeira 23/10/2020 19:41:40

Documento assinado digitalmente por:
Marcos Flavio Nascimento Maia 31/10/2020 10:06:58

1.9 **DE PROJETO E DE IMPLEMENTAÇÃO**

1.9.1 Não se aplica.

1.10 DE IMPLANTAÇÃO

1.10.1 O serviço de implantação poderá ser executado presencialmente na Sede do TRE/RN ou remotamente, acompanhados e supervisionados por sua equipe técnica e realizados prioritariamente durante o expediente normal da Justiça Eleitoral do Rio Grande do Norte.

1.10.1.1 Caso necessário, visando minimizar o impacto para os usuários, o TRE/RN poderá exigir a execução da implantação fora do horário de expediente normal, ou seja, durante a noite, a madrugada ou em finais de semana e feriado.

1.11 DE GARANTIA E MANUTENÇÃO

1.11.1 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.

1.11.1.1 O suporte pelo fabricante será obrigatório.

1.11.1.2 O suporte pela fornecedora da solução será opcional e ela poderá subcontratar uma empresa autorizada pelo fabricante para prestar o suporte técnico de primeiro nível.

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

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

1.11.4 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.

1.11.5 A empresa deve possuir, no momento da assinatura do contrato, pelo menos **01 (um)** profissional com certificação técnica emitida pelo fabricante, capaz de prestar o serviço especializado de instalação e configuração da solução.

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

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

1.11.6.1.1 Não poderá ser superior a **02 (duas) horas**, após abertura do chamado, para problemas com severidade crítica (funcionalidade do produto completamente degradada, impacto crítico nas operações).

Documento assinado digitalmente por:		
FRANCISCO DE A. PAIVA LEAL:92440776 23/10/2020 18:57:47	DENILSON BASTOS DA SILVA:20024241 23/10/2020 19:21:28	Marat Soares Teixeira 23/10/2020 19:41:40

Documento assinado digitalmente por:
Marcos Flavio Nascimento Maia 31/10/2020 10:06:58

1.11.6.1.2 Não poderá ser superior a **12 (doze) horas**, após abertura do chamado, para problemas com severidade alta (funcionalidade do produto severamente degradada, impacto severo nas operações).

1.11.6.1.3 Não poderá ser superior a **02 (dois) dias úteis**, após abertura do chamado, para problemas com severidade média (erros, problemas gerais, produto danificado, no entanto, as operações permanecem funcionais).

1.11.7 A empresa fornecedora da solução ou o fabricante deverão disponibilizar, cumulativamente, abertura de suporte técnico por meio de atendimento telefônico, *website e e-mail.*

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

1.11.9 A fornecedora da solução ou o fabricante deverão disponibilizar um portal web com disponibilidade de 24 (vinte e quatro) horas por dia, 07(sete) dias por semana e 365 (trezentos e sessenta e cinco) dias por ano, com sistema de *help-desk* para abertura de chamados de suporte técnico.

1.11.10 A equipe técnica do TRE/RN poderá abrir, gerenciar status e conferir todo o histórico de chamados de suporte técnico, mediante *login* e senha de acesso ao sistema.

1.11.11 Os chamados abertos por e-mail deverão ter sua abertura automática no portal *web*.

1.11.12 Todo o chamado aberto deverá ter sua resolução técnica registrada no sistema *web* de *help-desk.*

1.11.13 O TRE/RN poderá solicitar o escalonamento de incidentes ao fabricante quando se tratarem de correções especiais, defeitos nos programas ou defeito em *hardware*.

1.11.14 A fornecedora da solução 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.

1.11.15 A garantia iniciará sua contagem a partir da data de emissão da nota fiscal dos *softwares*, serviços ou licenças.

1.11.16 Havendo discrepâncias entre o que está especificado no item específico e o que consta nestas condições gerais, prevalecerá o que está no item específico.

1.11.17 A fornecedora da solução 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 (36 meses, a depender da garantia explicitada para o item em questão), sem qualquer ônus adicional para o contratante.

1.11.18 As atualizações incluídas devem ser do tipo "*minor release*" e "*major release*", permitindo manter todos componentes atualizados em sua última versão de *software/firmware*.

Documento assinado digitalmente por:		
FRANCISCO DE A. PAIVA LEAL:92440776 23/10/2020 18:57:47	DENILSON BASTOS DA SILVA:20024241 23/10/2020 19:21:28	Marat Soares Teixeira 23/10/2020 19:41:40

Documento assinado digitalmente por:
Marcos Flavio Nascimento Maia 31/10/2020 10:06:58

1.12 DE CAPACITAÇÃO

1.12.1 Deverá ser realizado o repasse tecnológico para a equipe técnica por meio presencial ou remotamente, com carga horária mínima de **20 (vinte) horas** e deverá abordar as informações necessárias à gerência, administração, auditoria e suporte interno da solução.

1.12.2 Além do repasse tecnológico para as equipes técnicas, deverão ser fornecidos documentos e tutoriais (em português) necessários à capacitação dos usurários finais da solução a respeito das funcionalidades da solução.

1.12.3 Ao término do repasse tecnológico, que terá o mínimo de **10 (dez) participantes**, deverão ser fornecidos atestados de participação, contendo no mínimo o nome do aluno, assunto, entidade promotora, carga horária, período de realização, ministrante e conteúdo programático.

1.13 DE EXPERIÊNCIA PROFISSIONAL DA EQUIPE QUE PROJETARÁ, IMPLEMENTARÁ E IMPLANTARÁ A SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

1.13.1 O profissional responsável pela implantação deverá apresentar documentação que ateste pelo menos **02 (dois) anos** de experiência de uso da ferramenta contratada.

1.13.1.1 Os serviços previstos objeto deste estudo preliminar deverão ser realizados por profissionais com perfis técnicos compatíveis com cada atividade, ou seja, por recursos especialistas habilitados, com base em cursos e certificações oficiais.

1.14 DE FORMAÇÃO DA EQUIPE QUE PROJETARÁ, IMPLEMENTARÁ E IMPLANTARÁ A SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

1.14.1 Não se aplica.

1.15 DE METODOLOGIA DE TRABALHO

1.15.1 Não se aplica.

Documento assinado digitalmente por:		
FRANCISCO DE A. PAIVA LEAL:92440776 23/10/2020 18:57:47	DENILSON BASTOS DA SILVA:20024241 23/10/2020 19:21:28	Marat Soares Teixeira 23/10/2020 19:41:40

Documento assinado digitalmente por:
Marcos Flavio Nascimento Maia 31/10/2020 10:06:58

1.16 DE SEGURANÇA DA INFORMAÇÃO

1.16.1 A fornecedora da solução deverá obedecer aos critérios, padrões, normas e procedimentos operacionais adotados pela JUSTIÇA ELEITORAL e, em especial, observar a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral, instituída através da Resolução no 23.501 de 19 de dezembro de 2016 do Tribunal Superior Eleitoral e a Política de Segurança da Informação (PSI), no âmbito do Tribunal Regional Eleitoral do Rio Grande do Norte, instituída através da Resolução n° 20/2019 de 11 de setembro de 2019, quanto aos seguintes aspectos:

1.16.1.1 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 Rio Grande do Norte aos quais tiver acesso em decorrência do objeto da presente contratação, ficando terminantemente proibida de fazer uso ou revelação destes sob qualquer justificativa.

1.16.1.2 O Tribunal Regional Eleitoral do Rio Grande do Norte terá propriedade sobre todos os documentos e procedimentos operacionais produzidos no escopo da presente contratação.

1.16.1.3 Os documentos eventualmente produzidos deverão ser repassados ao TRE/RN tanto em formato não editável (*PDF*) como também em formato editável (.*DOCX* ou .*ODT*).

1.16.2 A fornecedora da solução deverá concordar que as informações a que terá acesso serão utilizadas somente nos processos envolvidos para execução do objeto contratado.

1.16.3 A fornecedora da solução se obriga a informar imediatamente ao TRE/RN qualquer violação das regras de sigilo ora estabelecidas que tenha ocorrido por sua ação ou omissão, independentemente da existência de dolo, bem como de seus empregados, prepostos e prestadores de serviço.

1.16.4 A solução deverá proporcionar a disponibilidade, a integridade e a segurança de todas as informações do TRE/RN por ela gerenciadas e armazenadas.

1.16.5 O acesso as ferramentas de colaboração e comunicação deverá ser feito através de conexão segura (*HTTPS*).

1.17 DE QUALIDADE

1.17.1 Não se aplica.

Documento assinado digitalmente por:		
FRANCISCO DE A. PAIVA LEAL:92440776 23/10/2020 18:57:47	DENILSON BASTOS DA SILVA:20024241 23/10/2020 19:21:28	Marat Soares Teixeira 23/10/2020 19:41:40

Documento assinado digitalmente por:
Marcos Flavio Nascimento Maia 31/10/2020 10:06:58

2 AVALIAÇÃO DE SOLUÇÕES

2.1 DISPONIBILIDADE DE SOLUÇÃO SIMILAR EM OUTRO ÓRGÃO OU ENTIDADE DA ADMINISTRAÇÃO PÚBLICA

2.1.1 Em consulta de mercado se observou que existem 03 (três) soluções capazes de prover o gerenciamento de vulnerabilidades, sem necessidade de aquisição de *hardwares* específicos, e que podem atender aos requisitos:

2.1.1.1 Utilização de ferramenta disponibilizada sob a modalidade de *softwares* livres (código aberto) ou de forma gratuita.

2.1.1.2 Utilização de ferramenta comercial com gerenciamento e armazenamento na nuvem (*On Cloud*).

2.1.1.3 Utilização de ferramenta comercial com gerenciamento e armazenamento na rede local do Tribunal (*On Premise*).

2.1.2 A tabela abaixo mostra alguns dos fornecedores da(s) solução(es):

Solução	Descrição	Fornecedor(es)
Gratuita	Ferramenta disponibilizada sob a modalidade de *softwares* livres (código aberto) ou de forma gratuita	- *OpenVas* - *Nmap*
Comercial (*On Cloud*)	Ferramenta de gerenciamento de vulnerabilidades e análise dinâmica de aplicações web baseado em nuvem, com modelo de subscrição por tempo determinado	- *Qualys* - *Tenable* - *Rapid7*
Comercial (*On Premise*)	Ferramenta 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 tempo determinado, ou de licença perpétua com suporte técnico por tempo determinado	- *Tenable* - *Rapid7*

2.1.3 As alternativas descritas nos itens 2.1.1.1, 2.1.1.2 e 2.1.1.3 referem-se à aquisição de *softwares* e encontram-se implantadas:

2.1.3.1 No Comando da Marinha – Dispensa de Licitação Nº 671/2018 renovação da assinatura do software Nessus da empresa *Tenable* por um período de 12 (doze) meses.

2.1.3.2 No Conselho da Justiça Federal – Processo SEI 0001989-89.2019.4.90.8000 – Pregão Eletrônico 01/2020 relata o uso só *software Rapid7*.

2.1.3.3 No Tribunal Regional Eleitoral do Paraná – Pregão Eletrônico 03/2020 – Empresa vencedora fornece a ferramenta *Qualys*.

2.1.3.4 No Banco do Estado do Rio Grande do Sul - Banrisul – Pregão Eletrônico 509/2019 – Empresa vencedora fornece o produto *Nessus* da empresa *Tenable*.

Documento assinado digitalmente por:		
FRANCISCO DE A. PAIVA LEAL:92440776 23/10/2020 18:57:47	DENILSON BASTOS DA SILVA:20024241 23/10/2020 19:21:28	Marat Soares Teixeira 23/10/2020 19:41:40

Documento assinado digitalmente por:
Marcos Flavio Nascimento Maia 31/10/2020 10:06:58

2.2 DISPONIBILIDADE SOLUÇÕES EXISTENTES NO PORTAL DO *SOFTWARE* PÚBLICO BRASILEIRO

2.2.1 Em consulta no Portal do Software Público Brasileiro não está disponível solução(ões) que atenda os requisitos.

2.3 CAPACIDADE E ALTERNATIVAS NO MERCADO DE TIC, INCLUSIVE A EXISTÊNCIA DE *SOFTWARE* LIVRE OU *SOFTWARE* PÚBLICO

2.3.1 Em consulta no mercado de TIC se observou a soluções capazes de prover o gerenciamento de vulnerabilidades, sem necessidade de aquisição de *hardwares* específicos, e que podem atender aos requisitos:

2.3.1.1 *OpenVAS* que é um *framework* de vários serviços e ferramentas que oferece uma solução de varredura e gerenciamento de vulnerabilidade.

2.3.1.2 *Nmap* que é um *software* livre que realiza *port scan,* muito utilizado para avaliar a segurança dos computadores e para descobrir serviços ou servidores em uma rede de computadores, conhecido pela sua rapidez e pelas opções que dispõe.

2.3.1.3 T*enable Nessus Vulnerability Scanner* é uma solução de avaliação de vulnerabilidades *On Cloud*.

2.3.1.3.1 Ela impede ataques de rede, identificando as vulnerabilidades e problemas de configuração que hackers usam para penetrar sua rede.

2.3.1.4 *Tenable Nessus Vulnerability Scanner* é uma solução de avaliação de vulnerabilidades *On Premisse*.

2.3.1.4.1 Ela impede ataques de rede, identificando as vulnerabilidades e problemas de configuração que *hackers* usam para penetrar sua rede.

2.3.1.5 O *Rapid7* é uma solução de gerenciamento de vulnerabilidade *On Cloud*.

2.3.1.5.1 O seu propósito é ajudar a reduzir sua exposição a ameaças, permitindo que você avalie e responda às mudanças em seu ambiente em tempo real e priorizando riscos em vulnerabilidades, configurações e controles.

2.3.1.6 O *Rapid7* é uma solução de gerenciamento de vulnerabilidade *On Premisse*.

2.3.1.6.1 O seu propósito é ajudar a reduzir sua exposição a ameaças, permitindo que você avalie e responda às mudanças em seu ambiente em tempo real e priorizando riscos em vulnerabilidades, configurações e controles.

2.3.1.7 O *Qualys Web Application Scanning (WAS)* é um serviço em nuvem que fornece rastreamento e testes automatizados de aplicativos *web* personalizados para identificar vulnerabilidades.

Documento assinado digitalmente por:		
FRANCISCO DE A. PAIVA LEAL:92440776 23/10/2020 18:57:47	DENILSON BASTOS DA SILVA:20024241 23/10/2020 19:21:28	Marat Soares Teixeira 23/10/2020 19:41:40

Documento assinado digitalmente por:
Marcos Flavio Nascimento Maia 31/10/2020 10:06:58

2.4 OBSERVÂNCIA ÀS POLÍTICAS, PREMISSAS E ESPECIFICAÇÕES TÉCNICAS DEFINIDAS PELOS MODELO NACIONAL DE INTEROPERABILIDADE DO PODER JUDICIÁRIO (MNI) E MODELO DE ACESSIBILIDADE DE GOVERNO ELETRÔNICO (E-MAG)

2.4.1 A solução a ser implantada não tem por finalidade a comunicação com outros órgãos do Poder Judiciário, portanto, não se aplica a observância ao Modelo Nacional de Interoperabilidade MNI.

2.4.2 A solução a ser implantada será acessível somente a determinados servidores do quadro deste regional, portanto, não se aplica a observância ao Modelo de Acessibilidade de Governo Eletrônico E-MAG.

2.5 OBSERVÂNCIA AOS REQUISITOS ESTABELECIDOS PELA RESOLUÇÃO CNJ Nº 211/2015 E ALTERAÇÕES POSTERIORES, NA CONTRATAÇÃO DE SERVIÇOS DE DESENVOLVIMENTO E DE SUSTENTAÇÃO DE SISTEMAS DE INFORMAÇÃO

2.5.1 Não se aplica.

2.6 ADERÊNCIA ÀS REGULAMENTAÇÕES DA INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRAS (ICP-BRASIL), QUANDO HOUVER NECESSIDADE DE UTILIZAÇÃO DE CERTIFICADO DIGITAL, OBSERVADA A LEGISLAÇÃO SOBRE O ASSUNTO

2.6.1 Não se aplica.

2.7 OBSERVÂNCIA ÀS ORIENTAÇÕES, PREMISSAS E ESPECIFICAÇÕES TÉCNICAS E FUNCIONAIS DEFINIDAS PELO MODELO DE REQUISITOS PARA SISTEMAS INFORMATIZADOS DE GESTÃO DE PROCESSOS E DOCUMENTOS DO PODER JUDICIÁRIO (MOREQ-JUS), DO CONSELHO NACIONAL DE JUSTIÇA – CNJ E PELO E-ARQ (NORMAS E PADRÕES DE ARQUIVOLOGIA)

2.7.1 Não se aplica.

Documento assinado digitalmente por:		
FRANCISCO DE A. PAIVA LEAL:92440776 23/10/2020 18:57:47	DENILSON BASTOS DA SILVA:20024241 23/10/2020 19:21:28	Marat Soares Teixeira 23/10/2020 19:41:40

Documento assinado digitalmente por:
Marcos Flavio Nascimento Maia 31/10/2020 10:06:58

2.8 ORÇAMENTO ESTIMADO QUE EXPRESSE A COMPOSIÇÃO DE TODOS OS CUSTOS UNITÁRIOS RESULTANTES DOS ITENS A SEREM CONTRATADOS, ELABORADO COM BASE EM PESQUISA FUNDAMENTADA DE PREÇOS, COMO OS PRATICADOS NO MERCADO DE TIC EM CONTRATAÇÕES SIMILARES REALIZADAS POR ÓRGÃOS OU ENTIDADES DA ADMINISTRAÇÃO PÚBLICA, ENTRE OUTROS PERTINENTES

2.8.1 Em consulta realizada em âmbito nacional para uma prévia comparação de custos, se obteve o seguinte:

Item	Fornecedor	Descrição/ Modelo	Quant. Prevista	Quant. Registrada	Valor Unitário	Valor Total
2.8.1.1	Comunidades	*Software* livre OpenVas	0	0	R$ 0,00	R$ 0,00
		Software livre *Nmap*	0	0	R$ 0,00	R$ 0,00
Total						**R$ 0,00**

Documento assinado digitalmente por:		
FRANCISCO DE A. PAIVA LEAL:92440776 23/10/2020 18:57:47	DENILSON BASTOS DA SILVA:20024241 23/10/2020 19:21:28	Marat Soares Teixeira 23/10/2020 19:41:40

Documento assinado digitalmente por:
Marcos Flavio Nascimento Maia 31/10/2020 10:06:58

Item	Fornecedor	Descrição/ Modelo	Quant. Prevista	Quant. Registrada	Valor Unitário	Valor Total
2.8.1.2	Qualys (*On Cloud*)	Licenciamento de plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando, no mínimo, **250 (duzentos e cinquenta) endereços *IPs***, por **36 (trinta e seis) meses** de uso e suporte do fabricante	1	1	R$ 137.826,00	R$ 137.826,00
		Licenciamento para solução de análise dinâmica em aplicações *Web*, pacote para, no mínimo, **05 (cinco) domínios** (*FQDN*), por **36 (trinta e seis) meses** de uso e suporte do fabricante	1	1	R$ 59.970,00	R$ 59.970,00
		Instalação e configuração	1	1	R$ 6.890,00	R$ 6.890,00
		Repasse tecnológico, com período mínimo de **20 (vinte) horas**	1	1	R$ 4.500,00	R$ 4.500,00
		04 (quatro) horas de serviço especializado	0	50	R$ 1.250,00	R$ 0,00
Total						**R$ 209.186,00**

Documento assinado digitalmente por:		
FRANCISCO DE A. PAIVA LEAL:92440776 23/10/2020 18:57:47	DENILSON BASTOS DA SILVA:20024241 23/10/2020 19:21:28	Marat Soares Teixeira 23/10/2020 19:41:40

Documento assinado digitalmente por:
Marcos Flavio Nascimento Maia 31/10/2020 10:06:58

Item	Fornecedor	Descrição/ Modelo	Quant. Prevista	Quant. Registrada	Valor Unitário	Valor Total
2.8.1.3	Rapid7 (*On Cloud*)	Licenciamento de plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando, no mínimo, **250 (duzentos e cinquenta) endereços *IPs***, por **36 (trinta e seis) meses** de uso e suporte do fabricante	1	1	R$ 155.375,00	R$ 155.375,00
		Licenciamento para solução de análise dinâmica em aplicações *Web*, pacote para, no mínimo, **05 (cinco) domínios** (*FQDN*), por **36 (trinta e seis) meses** de uso e suporte do fabricante	1	1	R$ 246.622,00	R$ 246.622,00
		Instalação e configuração e repasse Tecnológico com período mínimo de **20 (vinte) horas**	1	1	R$ 38.000,00	R$ 38.000,00
		Repasse tecnológico, com período mínimo de **20 (vinte) horas**	1	1	R$ 10.000,00	R$ 10.000,00
		Banco de **04 (quatro) horas** técnicas (*on demand*) 100% REMOTO em regime de atendimento 8x5	0	1	R$ 1.000,00	R$ 1.000,00
Total						**R$ 450.997,00**

Documento assinado digitalmente por:		
FRANCISCO DE A. PAIVA LEAL:92440776 23/10/2020 18:57:47	DENILSON BASTOS DA SILVA:20024241 23/10/2020 19:21:28	Marat Soares Teixeira 23/10/2020 19:41:40

Documento assinado digitalmente por:
Marcos Flavio Nascimento Maia 31/10/2020 10:06:58

Item	Fornecedor	Descrição/ Modelo	Quant. Prevista	Quant. Registrada	Valor Unitário	Valor Total
2.8.1.4	*Tenable* (*On Cloud*)	Licenciamento de plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando, no mínimo, **250 (duzentos e cinquenta) endereços *IPs***, por **36 (trinta e seis) meses** de uso e suporte do fabricante	1	1	R$ 158.250,00	R$ 158.250,00
		Licenciamento para solução de análise dinâmica em aplicações *Web*, pacote para, no mínimo, **05 (cinco) domínios** (*FQDN*), por **36 (trinta e seis) meses** de uso e suporte do fabricante	1	1	R$ 64.710,00	R$ 64.710,00
		Instalação e configuração e repasse Tecnológico com período mínimo de **20 (vinte) horas**	1	1	R$ 11.322,00	R$ 11.322,00
		Repasse tecnológico, com período mínimo de **20 (vinte) horas**	1	1	R$ 8.342,00	R$ 8.342,00
		04 (quatro) horas de serviço especializado	0	50	R$ 0,00	R$ 0,00
		Total				**R$ 242.624,00**

Documento assinado digitalmente por:		
FRANCISCO DE A. PAIVA LEAL:92440776 23/10/2020 18:57:47	DENILSON BASTOS DA SILVA:20024241 23/10/2020 19:21:28	Marat Soares Teixeira 23/10/2020 19:41:40

Documento assinado digitalmente por:
Marcos Flavio Nascimento Maia 31/10/2020 10:06:58

Item	Fornecedor	Descrição/ Modelo	Quant. Prevista	Quant. Registrada	Valor Unitário	Valor Total
2.8.1.5	*Rapid7* (*On Premise*)	Licenciamento de plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando no mínimo **250 (duzentos e cinquenta) endereços IPs**, por **36 (trinta e seis) meses** de uso e suporte do fabricante	1	1	R$ 155.375,00	R$ 155.375,00
		Licenciamento para solução de análise dinâmica em aplicações *Web*, pacote para no mínimo **05 (cinco) domínios** (FQDN), por **36 (trinta e seis) meses** de uso e suporte do fabricante	1	1	R$ 369.933,75	R$ 369.933,75
		Instalação e configuração e repasse Tecnológico com período mínimo de **20 (vinte) horas**	1	1	R$ 38.000,00	R$ 38.000,00
		Repasse Tecnológico com período mínimo de **20 (vinte) horas**	1	1	R$ 10.000,00	R$ 10.000,00
		Banco de **04 (quatro) horas** técnicas (*on demand*) 100% REMOTO em regime de atendimento 8x5	0	1	R$ 1.000,00	R$ 1.000,00
		Total				**R$ 574.308,75**

Documento assinado digitalmente por:		
FRANCISCO DE A. PAIVA LEAL:92440776 23/10/2020 18:57:47	DENILSON BASTOS DA SILVA:20024241 23/10/2020 19:21:28	Marat Soares Teixeira 23/10/2020 19:41:40

Documento assinado digitalmente por:
Marcos Flavio Nascimento Maia 31/10/2020 10:06:58

Item	Fornecedor	Descrição/ Modelo	Quant. Prevista	Quant. Registrada	Valor Unitário	Valor Total
2.8.1.6	*Tenable* (*On Premise*)	Licenciamento de plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando no mínimo **250 (duzentos e cinquenta) endereços *IPs***, por **36 (trinta e seis) meses** de uso e suporte do fabricante	1	1	R$ 145.650,96	R$ 145.650,96
		Licenciamento para solução de análise dinâmica em aplicações Web, pacote para no mínimo **05 domínios** (**FQDN**), por **36 (trinta e seis) meses** de uso e suporte do fabricante	1	1	R$ 0,00	R$ 0,00
		Instalação e configuração	1	1	R$ 11.322,00	R$ 11.322,00
		Repasse Tecnológico com período mínimo de **20 (vinte) horas**	1	1	R$ 8.342,00	R$ 8.342,00
		04 (quatro) horas de Serviço Especializado	0	50	R$ 0,00	R$ 0,00
		Total				**R$ 165.314,96**

Documento assinado digitalmente por:		
FRANCISCO DE A. PAIVA LEAL:92440776 23/10/2020 18:57:47	DENILSON BASTOS DA SILVA:20024241 23/10/2020 19:21:28	Marat Soares Teixeira 23/10/2020 19:41:40

Documento assinado digitalmente por:
Marcos Flavio Nascimento Maia 31/10/2020 10:06:58

3 ESCOLHA E JUSTIFICATIVA DA SOLUÇÃO

3.1 **A solução escolhida foi a alternativa descrita:**

3.1.1 No **item 2.8.1.6** fornecida pela empresa *Tenable*.

3.1.1.1 Esta solução é baseada no gerenciamento em rede local do TRE/RN, possui o menor preço dentre os itens apresentados e atende todos os requisitos já elencados.

3.2 **Justificativa da escolha:**

3.2.1 Após avaliarmos as soluções contidas no **item 2.8.1**, podemos justificar a nossa escolha com base nos seguintes argumentos:

3.2.1.1 As soluções contidas no **item 2.8.1.1** são baseadas em *software* livre e atendem apenas parte da necessidade, pois a utilização desse cenário implica em não contar com suporte técnico especializado.

3.2.1.1.1 Além disso, a atualização da base de vulnerabilidades e falhas não possui a mesma frequência de cenários com softwares pagos.

3.2.1.1.2 Outro ponto desfavorável ao uso desses *softwares* é que os relatórios fornecidos pelas ferramentas não apresentam rastreabilidade das atividades já realizadas nos ativos e sistemas.

3.2.1.2 As soluções contidas nos **itens 2.8.1.2, 2.8.1.3** e **2.8.1.4** são baseadas em nuvem (*cloud computing*) e apresentam facilidade de gerenciamento, valor de aquisição adequado e facilidade nas atualizações da solução que serão todas feitas pelo fabricante.

3.2.1.2.1 Todos os requisitos de funcionalidades do projeto são atendidos por esse cenário.

3.2.1.2.2 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*.

3.2.1.2.3 Porém como os dados armazenados pela ferramenta (vulnerabilidades dos ativos de TIC) são muito sensíveis não é recomendável estarem armazenados em nuvem pública.

3.2.1.3 As soluções contidas nos **itens 2.8.1.5** e **2.8.1.6** são baseadas no gerenciamento em rede local do TRE/RN (*On Premise*).

3.2.1.3.1 A solução fornecida pela *Tenable* apresenta um valor de aquisição adequado e menor do que a solução que consta no **item 2.8.1.4** (*On Cloud*).

3.2.1.3.1.1 Apesar do **item 2.8.1.6** (*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.

3.2.1.3.1.2 Todas os requisitos de funcionalidades do projeto também são atendidos por esse cenário.

3.2.1.3.1.3 As soluções analisadas *Tenable* e *Rapid7* conseguem fazer o gerenciamento de vulnerabilidades em ativos de tecnologia da informação além de testes em aplicações *Web*.

Documento assinado digitalmente por:		
FRANCISCO DE A. PAIVA LEAL:92440776 23/10/2020 18:57:47	DENILSON BASTOS DA SILVA:20024241 23/10/2020 19:21:28	Marat Soares Teixeira 23/10/2020 19:41:40

Documento assinado digitalmente por:
Marcos Flavio Nascimento Maia 31/10/2020 10:06:58

3.2.1.3.1.4 Outro ponto favorável ao **item 2.8.1.6** fornecido pela *Tenable* é o fato de que após o término do suporte, a STIE continuará a ter acesso a ferramenta embora sem o direito de recebimento de atualizações de versão e de novas vulnerabilidades.

3.2.1.4 **Atualmente está em curso no Tribunal Regional Eleitoral da Paraíba, com apoio de outros Regionais, um registro de preços para a contratação de ferramenta de gestão de vulnerabilidades, que atende a todos os requisitos elencados neste estudo, onde o processo está bem avançado e que se configuraria a solução mais vantagosa, caso o TRE/RN optasse por participar do referido registro de preços.**

3.3 **A solução está alinhada:**

3.3.1 Às necessidades de negócio e requisitos tecnológicos.

3.3.2 **Necessidade de alcance dos seguintes objetivos estratégicos, elencados no:**

3.3.2.1 **Plano Estratégico da Justiça Eleitoral do RN 2016-2020 (PEJERN):**

3.3.2.1.1 Aprimorar a infraestrutura, a gestão e a governança de Tecnologia da Informação e Comunicação (TIC) – Objetivo Estratégico nº 9 (nove).

3.3.2.2 **Plano Estratégico de Tecnologia da Informação e Comunicação 2016-2020 (PETIC):**

3.3.2.2.1 Aperfeiçoar a segurança da informação e comunicação – Objetivo Estratégico nº 05 (cinco). .

3.3.2.2.2 Primar pela satisfação dos usuários de Tecnologia da Informação e Comunicação (TIC) – Objetivo Estratégico nº 06 (seis).

3.4 **A solução escolhida permitirá:**

3.4.1 Identificar as vulnerabilidades dos ativos de tecnologia da informação utilizados no TRE/RN.

3.4.2 Definir o grau de risco de cada ativo de acordo com as áreas de negócio.

3.4.3 Priorizar as ações necessárias à mitigação de riscos e correção das vulnerabilidades.

3.5 **A solução é composta por *softwares*:**

3.5.1 Atualmente existe a necessidade de aquisição de ferramenta de gestão de vulnerabilidades, conforme abaixo:

Item	Descrição	Tipo
1	Licenciamento de plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando, no mínimo, **250 (duzentos e cinquenta) endereços IPs**, por **36 (trinta e seis) meses** de uso e suporte do fabricante	*Tenable.sc Vulnerability Management*
2	Licenciamento para solução de análise dinâmica em aplicações *Web*, pacote para, no mínimo, **05 (cinco) domínios** (FQDN), por **36 (trinta e seis) meses** de uso e suporte do fabricante	*Tenable Web Application Scanning*

Documento assinado digitalmente por:		
FRANCISCO DE A. PAIVA LEAL:92440776 23/10/2020 18:57:47	DENILSON BASTOS DA SILVA:20024241 23/10/2020 19:21:28	Marat Soares Teixeira 23/10/2020 19:41:40

Documento assinado digitalmente por:
Marcos Flavio Nascimento Maia 31/10/2020 10:06:58

3	Instalação e configuração	-
4	Repasse tecnológico	Por um período mínimo de **20 (vinte) horas**
5	Suporte técnico	**04 (quatro) horas** de serviço especializado

3.6 **Os valores estimados estão descritos no item 2.8.1.**

3.7 **Os benefícios gerados são:**

3.7.1 Reduzir o nível de risco do ambiente de TIC por meio da correção das vulnerabilidades identificadas.

3.7.2 Proteger a informação e os ativos de tecnologia da informação utilizados no TRE/RN.

3.7.3 Garantir a disponibilidade dos sistemas que sustentam os serviços essenciais e a continuidade dos serviços oferecidos e uso das aplicações desenvolvidas e utilizadas pela Justiça Eleitoral.

3.7.4 Manter uma infraestrutura tecnológica compatível com as necessidades do TRE/RN, objetivando a busca contínua pela melhoria da qualidade e o padrão de excelência na prestação de serviços ao público interno e externo.

3.8 Relação Demanda Prevista x Quantidade de Bens Pretendidos (memória de cálculo):

3.8.1 Atualmente, considerando o aspecto orçamentário, a necessidade será atendida pela contratação de licenças do(s) seguinte(s) *software(s)*, na(s) quantidade(s) indicada(s):

Descrição	Quant. Atual	Quant. Necessária (Projeção)	Quant. para Aquisição
Licenciamento de plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando, no mínimo, **250 (duzentos e cinquenta) endereços *IPs***, por **36 (trinta e seis) meses** de uso e suporte do fabricante.	0	01	01
Licenciamento para solução de análise dinâmica em aplicações Web, pacote para, no mínimo, **05 (cinco) domínios** (*FQDN*), por **36 (trinta e seis) meses** de uso e suporte do fabricante.	0	01	01

Documento assinado digitalmente por:		
FRANCISCO DE A. PAIVA LEAL:92440776 23/10/2020 18:57:47	DENILSON BASTOS DA SILVA:20024241 23/10/2020 19:21:28	Marat Soares Teixeira 23/10/2020 19:41:40

Documento assinado digitalmente por:
Marcos Flavio Nascimento Maia 31/10/2020 10:06:58

4 NECESSIDADES DE ADEQUAÇÃO DO AMBIENTE

4.1 Não existe necessidade de adequação do ambiente para a execução contratual.

II – SUSTENTAÇÃO DA CONTRATAÇÃO

5 DEFINIÇÃO DE RECURSOS HUMANOS E MATERIAIS

5.1 IDENTIFICAÇÃO DOS RECURSOS HUMANOS NECESSÁRIOS À IMPLANTAÇÃO DA SOLUÇÃO

5.1.1 Representante Técnico na licitação

5.1.1.1 Francisco de Assis Paiva Leal

5.1.1.2 Responsabilidades:

5.1.1.2.1 Apoiar o pregoeiro durante todo processo licitatório

5.1.1.2.2 Responder os questionamentos dos licitantes durante o certame.

5.1.2 Técnico Segurança da Informação

5.1.2.1 Francisco de Assis Paiva Leal.

5.1.2.2 Responsabilidades:

5.1.2.2.1 Analisar se todos requisitos técnicos exigidos foram atendidos durante o processo de entrega da solução.

5.1.2.2.2 Monitorar a solução no estagio de produção.

5.1.2.2.3 Acionar o suporte de garantia quando necessário.

5.1.3 Equipe de Recebimento

5.1.3.1 Seção de Segurança da Informação

5.1.3.2 Responsabilidades:

5.1.3.2.1 Monitorar a entrega da solução quanto ao prazo e os requisitos técnicos e administrativos.

5.2 IDENTIFICAÇÃO DOS RECURSOS MATERIAIS NECESSÁRIOS À IMPLANTAÇÃO DA SOLUÇÃO

5.2.1 Não foi identificada a necessidade de recursos materiais adicionais para garantir a implantação da solução.

5.3 IDENTIFICAÇÃO DOS RECURSOS HUMANOS NECESSÁRIOS À CONTINUIDADE DA SOLUÇÃO

5.3.1 Não foi identificada a necessidade de recursos humanos adicionais para garantir a continuidade da solução.

Documento assinado digitalmente por:		
FRANCISCO DE A. PAIVA LEAL:92440776 23/10/2020 18:57:47	DENILSON BASTOS DA SILVA:20024241 23/10/2020 19:21:28	Marat Soares Teixeira 23/10/2020 19:41:40

Documento assinado digitalmente por:
Marcos Flavio Nascimento Maia 31/10/2020 10:06:58

5.4 IDENTIFICAÇÃO DOS RECURSOS MATERIAIS NECESSÁRIOS À CONTINUIDADE DA SOLUÇÃO

5.4.1 Não foi identificada a necessidade de recursos materiais adicionais para garantir a continuidade da solução.

5.5 IDENTIFICAÇÃO DA EQUIPE DE APOIO À LICITAÇÃO NECESSÁRIA À CONTINUIDADE DA SOLUÇÃO

5.5.1 A equipe de apoio à licitação necessária à continuidade da solução será composta por:

Nome do Servidor	Unidade de Lotação	Papel desempenhado
Francisco de Assis Paiva Leal	SSI/COINF/STIE	Integrante Técnico
Marat Soares Teixeira	SELIC/COLIC/SAOF	Integrante Administrativo
Denílson Bastos da Silva	SSI/COINF/STIE	Auxiliar Técnico
Helder Jean Brito da Silva	SSI/COINF/STIE	Auxiliar Técnico
Daniel César Gurgel Coelho Ponte	SRI/COINF/STIE	Auxiliar Técnico
João Paulo de Araújo Bezerra	SRI/COINF/STIE	Auxiliar Técnico

6 DEFINIÇÃO DAS ATIVIDADES DE TRANSIÇÃO E ENCERRAMENTO DA CONTRATAÇÃO

6.1 Não se aplica.

Documento assinado digitalmente por:		
FRANCISCO DE A. PAIVA LEAL:92440776 23/10/2020 18:57:47	DENILSON BASTOS DA SILVA:20024241 23/10/2020 19:21:28	Marat Soares Teixeira 23/10/2020 19:41:40

Documento assinado digitalmente por:
Marcos Flavio Nascimento Maia 31/10/2020 10:06:58

7 ELABORAÇÃO DE ESTRATÉGIA DE INDEPENDÊNCIA

7.1 TRANSFERÊNCIA DE CONHECIMENTO TECNOLÓGICO

7.1.1 Não se aplica.

7.2 DIREITOS DE PROPRIEDADE INTELECTUAL E AUTORAIS

7.2.1 Não se aplica.

7.3 DOCUMENTAÇÃO E AFINS PERTINENTES À TECNOLOGIA DE CONCEPÇÃO, MANUTENÇÃO, ATUALIZAÇÃO E CÓDIGO FONTE

7.3.1 Não se aplica.

Documento assinado digitalmente por:		
FRANCISCO DE A. PAIVA LEAL:92440776 23/10/2020 18:57:47	DENILSON BASTOS DA SILVA:20024241 23/10/2020 19:21:28	Marat Soares Teixeira 23/10/2020 19:41:40

Documento assinado digitalmente por:
Marcos Flavio Nascimento Maia 31/10/2020 10:06:58

III – ANÁLISE DE RISCOS

8 IDENTIFICAÇÃO DOS RISCOS

8.1 RISCOS DO PROCESSO DE CONTRATAÇÃO

Risco	**8.1.1 Indisponibilidade Orçamentária**	**Probabilidade:**	**MÉDIA**
Item	Dano		Impacto:
1	Não contratação imediata da solução		**ALTO**
2	Atraso no cronograma		**MÉDIO**
Ações de Prevenção/Contingência e Responsáveis			
Item	**Preventiva**		**Responsável**
1	Verificar e confirmar previamente disponibilidade orçamentária para a contratação da solução pretendida		STIE
2	Encaminhar em tempo hábil proposta de dotação orçamentária ao Órgão Ordenador de Despesas com previsão e prazo para a contratação da solução		STIE
Item	**Corretiva**		**Responsável**
1	Solicitar o remanejamento de recursos para atender temporariamente o serviço objeto do Termo de Referência		STIE

Risco	8.1.1 **Atraso no Trâmite Processual**	**Probabilidade:**	**MÉDIA**
Item	**Dano**		**Impacto:**
1	Atraso na contratação da solução		**MÉDIO**
2	Atraso no cronograma		**MÉDIO**
Ações de Prevenção/Contingência e Responsáveis			
Item	**Preventiva**		**Responsável**
1	Finalizar o Termo de Referência e documentos acessórios respeitando o cronograma previamente definido		Equipe de Planejamento da Contratação
2	Comunicar à Administração da criticidade do objeto contratado e da necessidade de agilidade na análise dos documentos e na tramitação do processo administrativo		STIE
Item	**Corretiva**		**Responsável**
1	Comunicar à Administração sobre a paralisação do processo durante a tramitação e solicitar prioridade na análise visando à conclusão do processo administrativo		STIE

Documento assinado digitalmente por:		
FRANCISCO DE A. PAIVA LEAL:92440776 23/10/2020 18:57:47	DENILSON BASTOS DA SILVA:20024241 23/10/2020 19:21:28	Marat Soares Teixeira 23/10/2020 19:41:40

Documento assinado digitalmente por:
Marcos Flavio Nascimento Maia 31/10/2020 10:06:58

Risco	8.1.2 **Impugnação Procedente**	**Probabilidade:**	**BAIXA**
Item	**Dano**		**Impacto:**
1	Interrupção do processo de contratação		**ALTO**
2	Atraso no cronograma		**ALTO**
3	Frustração da contratação		**ALTO**
Ações de Prevenção/Contingência e Responsáveis			
Item	**Preventiva**		**Responsável**
1	Elaboração de Estudos Preliminares e Termo de Referências consistentes que permitam assegurar a contratação		Equipe de Planejamento da Contratação
2	Revisar o Termo de Referência e certificar que o mesmo não possua cláusulas que restrinjam, sem a devida justificativa técnica, a participação de interessados ou que, de alguma forma, deixem um licitante em situação privilegiada para concorrer		Equipe de Planejamento da Contratação
3	Submeter, para análise, o Termo de Referência à Administração		Equipe de Planejamento da Contratação
4	Atendimento imediato por parte do suporte técnico a fim de responder, tempestivamente, os pedidos de esclarecimentos e impugnações apresentadas		Equipe de Planejamento da Contratação
Item	**Corretiva**		**Responsável**
1	Adequação do Termo de Referência, corrigindo os itens que foram motivos de impugnação, para viabilizar a reabertura do certame.		Equipe de Planejamento da Contratação
2	Promover a reabertura da licitação		Área Administrativa

Documento assinado digitalmente por:		
FRANCISCO DE A. PAIVA LEAL:92440776 23/10/2020 18:57:47	DENILSON BASTOS DA SILVA:20024241 23/10/2020 19:21:28	Marat Soares Teixeira 23/10/2020 19:41:40

Documento assinado digitalmente por:
Marcos Flavio Nascimento Maia 31/10/2020 10:06:58

Risco	8.1.3 **Licitação Frustrada (Deserta/Fracassada)**	**Probabilidade:**	**BAIXA**
Item	**Dano**		**Impacto:**
1	Interrupção do processo de contratação		**ALTO**
2	Atraso no cronograma		**ALTO**
3	Frustração da contratação		**ALTO**
Ações de Prevenção/Contingência e Responsáveis			
Item	**Preventiva**		**Responsável**
1	Promover análise de mercado com o objetivo de elencar as empresas que prestam serviço do objeto		Equipe de Planejamento da Contratação
2	Dar a devida publicidade ao certame licitatório		Área Administrativa
3	Evitar exigências técnicas demasiadamente restritivas e desnecessárias		Equipe de Planejamento da Contratação
4	Mensurar o preço global do serviço a ser contratado através de estudo minucioso, com pesquisa de preços na Internet, bem como com prestadores de serviço do ramo		Equipe de Planejamento da Contratação
Item	**Corretiva**		**Responsável**
1	Adequação do Termo de Referência para a realização de novo certame		Equipe de Planejamento da Contratação
2	Promover nova licitação		Área Administrativa
3	Pesquisa de Preços, caso necessário		Equipe de Planejamento da Contratação
4	Contratação Direta		Área Administrativa

Documento assinado digitalmente por:		
FRANCISCO DE A. PAIVA LEAL:92440776 23/10/2020 18:57:47	DENILSON BASTOS DA SILVA:20024241 23/10/2020 19:21:28	Marat Soares Teixeira 23/10/2020 19:41:40

Documento assinado digitalmente por:
Marcos Flavio Nascimento Maia 31/10/2020 10:06:58

Risco	8.1.4 **Licitação Anulada**	**Probabilidade:**	**BAIXA**
Item	**Dano**		**Impacto:**
1	Interrupção do processo de contratação		**ALTO**
2	Atraso no cronograma		**ALTO**
3	Frustração da contratação		**ALTO**
Ações de Prevenção/Contingência e Responsáveis			
Item	**Preventiva**		**Responsável**
1	Na elaboração do Termo de Referência observar se não existe vício de legalidade		Equipe de Planejamento da Contratação
2	Observar adequada publicidade da licitação		Área Administrativa
Item	**Corretiva**		**Responsável**
1	Adequação das exigências normativas sobre o objeto/procedimento licitatório		Equipe de Planejamento da Contratação
2	Promover a publicidade adequada à modalidade de licitação escolhida		Área Administrativa

Documento assinado digitalmente por:		
FRANCISCO DE A. PAIVA LEAL:92440776 23/10/2020 18:57:47	DENILSON BASTOS DA SILVA:20024241 23/10/2020 19:21:28	Marat Soares Teixeira 23/10/2020 19:41:40

Documento assinado digitalmente por:
Marcos Flavio Nascimento Maia 31/10/2020 10:06:58

8.2 RISCOS DA SOLUÇÃO DE TID (GESTÃO E EXECUÇÃO CONTRATUAL)

Risco	**8.2.1 Solução considerada inadequada pela área requisitante**	**Probabilidade:**	**BAIXA**
Item	**Dano**		**Impacto:**
1	Insatisfação dos usuários dos serviços de TIC		**ALTO**
2	Não utilização da solução		**ALTO**
3	Necessidade de nova avaliação da solução		**MÉDIO**
Ações de Prevenção/Contingência e Responsáveis			
Item	**Preventiva**		**Responsável**
1	Envolver o usuário/unidade requisitante na participação em todas as fases da contratação		STIE e SAOF
2	Nomear servidores experientes e capacitados para executar a fase de levantamento de requisitos da solução de TIC		STIE
Item	**Corretiva**		**Responsável**
1	Nomear nova Equipe de Planejamento da Contratação, substituindo a atual, para a elaboração de novo Termo de Referência visando a contratação de solução de TIC adequada a solicitação da área demandante		Área Administrativa
2	Nomear equipe ou realocar servidores do TRE/RN com o objetivo de auxiliar ou assumir, provisoriamente, a operação dos serviços prestados pela equipe da fornecedora da solução		STIE
3	Refazer o levantamento de requisitos junto ao usuário/unidade requisitante		STIE
4	Proceder com as alterações necessárias, na medida do possível, na solução de TIC fornecedora da solução, com objetivo de readequar e reimplantar a solução		STIE

Documento assinado digitalmente por:		
FRANCISCO DE A. PAIVA LEAL:92440776 23/10/2020 18:57:47	DENILSON BASTOS DA SILVA:20024241 23/10/2020 19:21:28	Marat Soares Teixeira 23/10/2020 19:41:40

Documento assinado digitalmente por:
Marcos Flavio Nascimento Maia 31/10/2020 10:06:58

Risco	**8.2.2 Não cumprimento do prazo de entrega do *software***	**Probabilidade:**	**BAIXA**
Item	Dano		Impacto:
1	Atraso na instalação da(s) licença(s)		**BAIXO**
Ações de Prevenção/Contingência e Responsáveis			
Item	**Preventiva**		**Responsável**
1	Consultar as empresas do ramo sobre adequação do prazo de entrega do software		STIE
2	Acompanhar rigorosamente junto à empresa o andamento da operação de entrega		Área Administrativa
Item	**Corretiva**		**Responsável**
1	Solicitar o fornecedor para a entrega imediata		Área Administrativa
2	Verificar as sanções cabíveis no caso do não cumprimento do prazo de entrega		Área Administrativa

Risco	**8.2.2 Entrega de software incompatível (especificações)**	**Probabilidade:**	**BAIXA**
Item	Dano		Impacto:
1	Ineficácia na execução dos serviços prestados pelo órgão		**ALTO**
Ações de Prevenção/Contingência e Responsáveis			
Item	**Preventiva**		**Responsável**
1	Verificar se o software está de acordo com as especificações mínimas exigidas no ato de entrega para fins de ateste provisório		STIE
Item	**Corretiva**		**Responsável**
1	Solicitar o fornecedor para a substituição do software incompatível		STIE
2	Informar o gestor da contratação sobre problemas contratuais de garantia		STIE

Documento assinado digitalmente por:		
FRANCISCO DE A. PAIVA LEAL:92440776 23/10/2020 18:57:47	DENILSON BASTOS DA SILVA:20024241 23/10/2020 19:21:28	Marat Soares Teixeira 23/10/2020 19:41:40

Documento assinado digitalmente por:
Marcos Flavio Nascimento Maia 31/10/2020 10:06:58

IV – CONCLUSÃO DOS ESTUDOS PRELIMINARES

9 DECLARAÇÃO DE VIABILIDADE

Em conformidade com o disposto no Manual de Contratações de Tecnologia da Informação e Comunicação, subitem 4.1.1.11, DECLARAMOS a viabilidade da contratação, com base no estudo realizado.

Natal/RN, *(datação eletrônica)*

Equipe de Planejamento da Contratação		
Integrante Demandante	**Integrante Técnico**	**Integrante Administrativo**
(assinado eletronicamente)	(assinado eletronicamente)	(assinado eletronicamente)
Denilson Bastos da Silva	**Francisco de Assis Paiva Leal**	**Marat Soares Teixeira**
SSI/COINF/STIE	SSI/COINF/STIE	SELIC/COLIC/SAOF

DENILSON BASTOS DA SILVA:20024241 Assinado de forma digital por DENILSON BASTOS DA SILVA:20024241 Dados: 2020.10.23 19:21:28 -03'00'

FRANCISCO DE ASSIS PAIVA LEAL:92440776 Assinado de forma digital por FRANCISCO DE ASSIS PAIVA LEAL:92440776 Dados: 2020.10.23 18:57:47 -03'00'

Documento assinado digitalmente por:		
FRANCISCO DE A. PAIVA LEAL:92440776 23/10/2020 18:57:47	DENILSON BASTOS DA SILVA:20024241 23/10/2020 19:21:28	Marat Soares Teixeira 23/10/2020 19:41:40

Documento assinado digitalmente por:
Marcos Flavio Nascimento Maia 31/10/2020 10:06:58

Despacho

1. Acolhendo o Parecer nº 1569/2020, AUTORIZO que este TRE/RN manifeste interesse em participar da IRP nº 22/2020-TRE/PB, em relação aos itens de nº 16, 20, 24, 25 e 26, **desde que a unidade demandante esteja ciente da ressalva constante do parágrafo 12 do aludido Parecer**.

2. Encaminhe-se os autos à unidade demandante (COINF) para ciência da ressalva constante do parágrafo 12 do referido Parecer da Assessoria Jurídica da Diretoria-Geral e manifestação em relação à manutenção do interesse na participação deste TRE/RN na referida licitação.

3. Em caso afirmativo, mantido o interesse na participação, encaminhem-se os autos à Seção de Análise Técnica das Contratações –SETEC para as providências cabíveis.

Yvette Bezerra Guerreiro Maia

Diretora-Geral

Yvette Bezerra Guerreiro Maia - 11/11/2020 18:10:19

Documento assinado digitalmente por:
Yvette Bezerra Guerreiro Maia 11/11/2020 18:10:19

Despacho

Ciente da Ressalva contida no parecer da AJDG, o interesse em participar da licitação permanece. À Seção de Análise Técnica das Contratações –SETEC para as providências cabíveis.

COINF/STIE, 12 de novembro de 2020.

Carlos Magno Do Rozario Camara - 12/11/2020 07:42:43

Documento assinado digitalmente por:
Carlos Magno do Rozario Camara 12/11/2020 07:42:59

TRIBUNAL REGIONAL ELEITORAL DE ALAGOAS
Avenida Aristeu de Andrade nº 377 - Bairro Farol - CEP 57051-090 - Maceió - AL

Estudos Preliminares

1. Análise de Viabilidade da Contratação (Resolução CNJ nº 182/2013 – Arts.12 e 14)

1.1. Contextualização

A área de Tecnologia da Informação e Comunicação - TIC - se tornou crítica para organizações de qualquer tamanho ou ramo de atuação. Assim, no âmbito do TRE/AL, qualquer perda de dados ou informações pode causar o comprometimento da imagem e dos serviços prestados por este órgão, com efeito interno e no atendimento ao público.

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.

2. Definição e Especificação dos Requisitos da Demanda (Art. 14, I)

2.1. Especificações Técnicas

Especificações Técnicas Mínimas:

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 maliciososconhecidos (malware) para no mínimo 250 IPs;
2. A solução deve possuir recurso de varredura ativa, onde o scanner comunica-se com os alvos (ativos) através darede;
3. A solução de gestão de vulnerabilidades deve suportar varreduras de dispositivos de IoT;
4. Deve ser capaz de identificar no mínimo 50.000 CVEs (Common Vulnerabilities and Exposures);
5. A solução deve ter a capacidade de adicionar etiquetas (tags) aos ativos de maneira automática, manual e possibilitaro uso de regras com parâmetros específicos para aplicação das mesmas;
6. Deve atribuir a todas as vulnerabilidades uma severidade baseada no CVSSv3 score;
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;
8. A solução deve fornecer criptografia de ponta a ponta dos dados de vulnerabilidades;
9. A solução deve possuir a capacidade de armazenar informações dos ativos descobertos no ambiente;
10. Deve possuir um sistema de busca de informações de um determinado ativo com no mínimos as seguintescaracterísticas:
    1. Por sistema operacional;

2. Por determinado software instalado;
3. Por Ativos impactados por determinada vulnerabilidade.

11. A solução deve possuir suporte para a adição de detecções personalizadas usando o OVAL (Open VulnerabilityAssessment Language);
12. Deve permitir aceitar o risco de uma determinada vulnerabilidade encontrada no ambiente;
13. Possibilitar alterar a criticidade de determinada vulnerabilidade de forma manual;
14. A solução deve possuir sistema de pontuação e priorização das vulnerabilidades;
15. A solução deve ser capaz de aplicar algoritmos de aprendizagem de máquina (machine learning) para analisar as características relacionadas a vulnerabilidades;
16. O sistema de pontuação e de priorização de vulnerabilidades deve avaliar no mínimo as seguintes características:
    1. CVSSv3 Impact Score;
    2. Idade da Vulnerabilidade;
    3. Se existe ameaça ou exploit que explore a vulnerabilidade;
    4. Número de produtos afetados pela vulnerabilidade;
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;
18. Deve possuir uma API para automação de processos e integração com aplicações terceiras permitindo, no mínimo, aextração de dados para carga no SIEM;
19. Deve possuir uma API para automação de processos e integração com aplicações ITSM do órgão para asvulnerabilidades encontradas, permitindo o agrupamento no chamado por ações corretivas;
20. A solução deve permitir a instalação de agentes em estações de trabalho e servidores, para varredura diretamenteno sistema operacional;
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.
22. A solução deve ser capaz de produzir relatórios nos seguintes formatos: PDF, CSV ou HTML;
23. A solução deve possuir recurso de monitoria passiva do tráfego de rede para identificação de anomalias, novosdispositivos e desvios de padrões observados;
24. A solução deve ser licenciada para o uso ilimitado de sensores passivos de rede para realizar o monitoramento emtempo real;
25. A solução deve possuir sensores, no mínimo, com as seguintes funcionalidades:
    1. Execução de verificação completa do sistema (rede), adequada para qualquer host;
    2. Verificação sem recomendações da rede, para que se possa personalizar totalmente as configurações da verificação;
    3. Autenticação de hosts e enumeração de atualizações ausentes;
    4. Execução de varredura simples para descobrir hosts ativos e portas abertas;
    5. Utilização de um scanner para verificar aplicativos da web;
    6. Avaliação de dispositivos móveis
    7. Auditoria de configuração de serviços em nuvem de terceiros;
    8. Auditoria de configuração dos gerenciadores de dispositivos móveis;
    9. Auditoria de configuração dos dispositivos de rede;
    10. Auditoria de configurações do sistema em relação a uma linha de base conhecida;
    11. Detecção de desvio de segurança Intel AMT;
    12. Verificação de malware nos sistemas Windows e Unix;
26. Deve ser possível determinar em tempo real quais portas de serviços (UDP/TCP) estão abertas em determinadoativo;
27. A solução deve ser capaz de realizar em tempo real a descoberta de novos ativos para no minímo:
    1. Bancos de dados;
    2. Hypervisors (no mímino VMWare ESX/ESXi);
    3. Dispositivos móveis;
    4. Dispositivos de rede;
    5. Endpoints;
    6. Aplicações;

28. A solução deve ser capaz de em tempo real detectar logins e downloads de arquivos em um compartilhamento derede;
29. Permitir identificar vulnerabilidades associadas a servidores SQL no tráfego de rede;
30. A solução deve possuir interface para integração com as principais soluções de SIEM de mercado, tais como IBMQRadar, Microfocus ArcSight e Splunk.
31. A solução deve possibilitar a realização de cópias de segurança, funcionamento em alta disponibilidade e criptografiade todos os dados armazenados, além de incluir todo o software e licenciamento necessários para o funcionamento completode acordo com as funcionalidades previstas neste Termo de Referência.
32. A atualização das ameaças deve ocorrer diariamente e sem interrupção dos serviços.
33. Configuração de segurança e acesso à gerência da solução:
    1. Todos os dados armazenados nos servidores da solução devem ser criptografados e possuir logs de acesso;
    2. Os dados em transito devem usar ao menos o algoritimo TLS 1.2 de chave 2048 bits;
    3. Os dados em transito devem ser criptografados ao menos com o algoritimo AES-128 bits;
    4. Os algoritimos de hash devem usar ao menos o algoritimo SHA-256;
    5. Será aceito como comprovação critérios de criptografia publicação em site do fabricante ou declaração do própriofabricante;
    6. Os dados armazenados devem ser criptografados ao menos com o algoritimo AES-256 bits;
    7. Somente servidores da Contratante ou pessoa por ela autorizada poderão ter acesso aos dados da solução;
    8. A solução deve permitir a criação de, no mínimo, 20 contas para gerência e acesso aos relatórios, sem custo adicional;
    9. A empresa contratada não deverá ter acesso a rede interna da contratante e todo trafego de dados deverá ser de saída einiciado pelos scanners (on-premises).
    10. Todas as licenças de uso de software devem ser registradas, na data da entrega, em nome da Contratante no site dofabricante.
34. Dos Relatórios:
    1. Deve ser capaz de executar relatórios periódicos de acordo com a frequência estabelecida pelo administrador, bemcomo a geração de relatórios sob demanda;
    2. A solução deve possibilitar a criação de relatórios baseados na seleção de ativos, permitindo inclusive a seleção detodos os ativos existentes;
    3. Deve suportar a criação de relatórios criptografados (protegidos por senha configurável);
    4. A solução deve suportar o envio automático de relatórios para destinatários específicos;
    5. Deve ser possível definir a frequência na geração dos relatórios para no mínimo: Diário, Mensal, Semanal e Anual;
    6. Permitir especificar níveis de permissão nos relatórios para usuários e grupos específicos;
    7. A solução deve fornecer relatórios do tipo “scorecard” para as partes interessadas da empresa;
    8. A solução deve fornecer relatórios de correções aplicadas, classificados pelos seguintes critérios: grupo de ativos,usuários e vulnerabilidades;
35. A solução deve permitir mecanismo de varredura baseado em inferência com técnicas de varredura não intrusivas;
36. A solução deve possuir ou permitir a criação de relatórios com as seguintes informações:
    1. Hosts verificados sem credenciais;
    2. Top 100 Vulnerabilidades mais criticas;
    3. Top 10 Hosts infectados por Malwares;
    4. Hosts exploráveis por Malwares;
    5. Total de vulnerabilidades que podem ser exploradas pelo Metasploit;
    6. Vulnerabilidades críticas e exploráveis;
    7. Máquinas com vulnerabilidades que podem ser exploradas;
37. A solução deve possuir dashboards customizáveis onde o administrador pode criar, editar ou remover painéis deacordo com a necessidade;
38. A solução deve ser capaz de inventariar todos os ativos da rede local e publicados na Internet, sem limites deendereços IPs.

39. A plataforma de software deve ser capaz de realizar varreduras (scans) de vulnerabilidades para no mínimo 250 IPs;
40. A plataforma de software deve ser licenciada para um número ilimitado de scanners (prevendo redundância);
41. Deve permitir a configuração de vários painéis e widgets;
42. Deve ser capaz de medir e reportar ameaças;
43. Deve ser capaz de visualizar ameaças críticas ao ambiente monitorado;
44. A plataforma de software deve realizar varreduras em uma variedade de sistemas operacionais, suportando pelomenos hosts baseados em Windows, Linux e Mac OS, bem como appliances virtuais;A plataforma de software deve suportar vários mecanismos de varredura distribuídos em diferentes localidades eregiões e gerenciar todos por uma console central;
45. A plataforma de software deve fornecer agentes instaláveis em sistemas operacionais, pelo menos Windows, Linux eMac OS, para o monitoramento contínuo de configurações e vulnerabilidades;
46. A plataforma de software deve permitir o monitoramento através de agentes instalados, até o limite de licençasadquiridas, para varredura diretamente no sistema operacional.
47. A plataforma de software deve permitir o monitoramento sem a necessidade de agentes instalados, até o limite delicenças adquiridas, para varredura diretamente no sistema operacional.
48. A plataforma de software deve incluir a capacidade de programar períodos de tempo e data onde varreduras nãopodem ser executadas, como por exemplo em determinados dias do mês ou determinados horários do dia;
49. No caso onde uma atividade de varredura seja interrompida por invadir o período não permitido, o mesmo deve sercapaz de ser reiniciado de onde parou;
50. A plataforma de software deve ser configurável para permitir a otimização das parametrizações de varredura;
51. A plataforma de software deve permitir a entrada e o armazenamento seguro de credenciais do usuário, incluindocontas locais, de domínio (LDAP e Active Directory) e root para sistemas Linux;

A plataforma de software deve fornecer a capacidade de escalar privilégios nos destinos, do acesso de usuáriopadrão até acesso de sistema ou administrativo;

1. A plataforma de software deve ser capaz de realizar pesquisas de dados confidenciais;
2. A solução deve possuir módulo para realizar análise dinâmica em aplicações Web:
3. 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:
4. A solução de análise deve ser capaz de analisar, testar e reportar falhas de segurança em aplicações Web;
5. A solução de análise deverá ser capaz de executar varreduras em sistemas Web através de seus endereços IP ouFQDN (DNS);
6. A solução de análise deve ser capaz de identificar vulnerabilidades de divulgação de dados, como vazamento deinformações de identificação pessoal;
7. Para varreduras do tipo extensas e detalhadas, deve varrer e auditar no mínimo os seguintes elementos:
    1. Cookies, Headers, Formulários e Links;
    2. Nomes e valores de parâmetros da aplicação;
    3. Elementos JSON e XML;
    4. Elementos DOM;
8. Deverá também permitir a execução da função crawler, que consiste na navegação para descoberta das URLsexistentes na aplicação;
9. A solução de análise deve suportar a integração com o softwares de automação de testes para permitir sequênciasde autenticação complexas;
10. A solução de análise deve ser capaz de realizar testes/varreduras em aplicações separadas, simultaneamentelimitadas ao número de licenças;
11. A solução de análise deve oferecer suporte à capacidade de testar novamente a vulnerabilidade específica que foidetectada anteriormente no aplicativo Web;
12. Deve ser capaz de utilizar scripts customizados de crawling com parâmetros definidos pelo usuário;

13. Deve ser capaz de excluir determinadas URLs da varredura através de expressões regulares;
14. Deve ser capaz de excluir determinados tipos de arquivos através de suas extensões;
15. Deve ser capaz de instituir no mínimo os seguintes limites:
    1. Número máximo de URLs para crawling e navegação;
    2. Número máximo de diretórios para varreduras;
    3. Número máximo de elementos DOM;
    4. Tamanho máximo de respostas;
    5. Tempo máximo para a varredura;
    6. Número máximo de conexões HTTP(S) ao servidor hospedando a aplicação Web;
    7. Número máximo de requisições HTTP(S) por segundo;
16. Deve ser capaz de agendar a varredura e determinar sua frequência entre uma única vez, diária, semanal,mensal e anual;
17. Deve suportar o envio de notificações por email;
18. Deverá ser compatível com avaliação de web services REST e SOAP;
19. A solução de análise deve suportar os seguintes esquemas de autenticação:
    1. Autenticação Básica (Digest);
    2. NTLM;
    3. Autenticação de Cookies;
20. Deve ser capaz de importar scripts de autenticação previamente configurados pelo usuário;
21. A solução de análise deve ser capaz de exibir os resultados das varreduras de forma temporal paraacompanhamento de correções e introdução de novas vulnerabilidades;
22. Os resultados devem ser apresentados agregados por vulnerabilidades ou por aplicações;
23. Para cada vulnerabilidade encontrada, deve ser exibido detalhes e evidências;
24. Cada vulnerabilidade encontrada deve conter também soluções propostas para mitigação ou remediação;
25. Serviço de Detecção de Malware:
    1. A solução de análise deve utilizar a plataforma de gerenciamento de vulnerabilidades existente;
    2. A solução de análise deve permitir visualizar o acompanhamento das atividades de verificação, páginas infectadas etendências de infecção por malware;
    3. A solução de análise deve fornecer relatórios de resumo geral de todas as aplicações web e resumo de uma aplicaçãoespecífica, que serão exportados para os formatos XML, HTML ou PDF.
26. A solução deve ser capaz de realizar varreduras nos seguintes componentes/aplicações:
    1. WordPress;
    2. IIS 6.x e IIS 10.x;
    3. ASP 6;
    4. NET 2;
    5. Apache HTTPD 2.2.x e 2.4.x;
    6. Tomcat 6.x, 7.x, 8.x e superiores;
    7. Jetty 8 e superiores;
    8. Nginx;
    9. PHP 5.3.x, 5.4.x, 5.6.x, 7.0.x e 7.1.x e superiores;
    10. Java 1.5, 1.6, 1.7 e 1.8 e superiores;
    11. Jboss 4.x e 7.x e superiores;
    12. WildFly 8 e 10 e superiores;
    13. Plone 2.5.x e 5.2.1.41.x e superiores;
    14. Zope;
    15. Python 2.4.4 e superiores;
    16. J2EE;
    17. Ansible;
    18. Joomla;
    19. Moodle;
    20. Docker Conteiner;
    21. Elk;
    22. GIT;
    23. Grafana; e

24. Redmine.

3. 3. Soluções Disponíveis no Mercado de TIC (Art. 14, I, a):

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

a. **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.

b. **Solução paga com gerenciamento e armazenamento na nuvem (On Cloud)**
   - Nome da Solução: Ferramenta de Gestão de Vulnerabilidades On Cloud
   - Possíveis Fornecedores: Qualys, Tenable, Rapid7, entre outros.
   - Descrição: Aquisição de software de gerenciamento de vulnerabilidades e análise dinâmica de aplicações web baseadoem nuvem, com modelo de subscrição por 36 meses.

c. **Solução paga com gerenciamento e armazenamento na rede local do Tribunal (On premise)**
   - Nome da Solução: Ferramenta de Gestão de Vulnerabilidades On premises
   - Possíveis Fornecedores: Tenable, Rapid7, entre outros.
   - Descrição: Aquisição de software de gerenciamento de vulnerabilidades e análise dinâmica de aplicações web baseadoem gerenciamento e armazenamento na rede local do tribunal, com modelo de subscrição por 36 meses ou de licençaperpetua com suporte de 36 meses.

4. Contratações Públicas Similares (Art. 14, I, b):

- Governo do Distrito Federal - Secretaria de Estado da Fazenda, Pregão Eletrônico 16/2018
- Ministério Público do Trabalho, Pregão de Eletrônico 21/2017
- Tribunal de Contas da União, Pregão Eletrônico 78/2018

5. Outras Soluções Disponíveis (Art. 14, II, a):

Não se aplica, smj, por se tratar de licenciamento e serviços de suporte padrão de mercado.

6. Portal do Software Público Brasileiro (Art. 14, II, b):

Não se aplica, smj, por se tratar de licenciamento e serviços de suporte padrão de mercado.

7. Alternativa no Mercado de TIC (Art. 14, II, c):

Não se aplica, smj, por se tratar de c licenciamento e serviços de suporte padrão de mercado.

8. Modelo Nacional de Interoperabilidade – MNI (Art. 14, II, d):

Não se aplica, smj, por se tratar de licenciamento e serviços de suporte padrão de mercado.

9. Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil (Art. 14, II, e):

Não se aplica, smj, por se tratar de licenciamento e serviços de suporte padrão de mercado.

10. Modelo de Requisitos Moreq-Jus (Art. 14, II, f):

Não se aplica, smj, por se tratar de licenciamento e serviços de suporte padrão de mercado.

11. Análise dos Custos Totais da Demanda (Art. 14, III):

Valor Estimado (baseado na melhor proposta da Tenable on premise): R$ 165.314,00 (Cento e sessenta e cinco mil trezentos e quatorze reais), com base nos valores obtidos em procedimento com o mesmo objeto em trâmite no TRE-PB, que terá como copartícipes vários outros TRE.

Eventos: 0782025, 0782027 e 0782030.

12. Escolha e Justificativa da Solução (Art. 14, IV):

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-AL 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.

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 36 meses ou de licença perpetua com suporte de 36 meses.

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.

13. Descrição da Solução (Art. 14, IV, a):

Contratação de solução de análise de vunerabilidades computacionais em servidores e serviços informatizados e serviços relacionados.

14. Alinhamento da Solução (Art. 14, IV, b):

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

15. Benefícios Esperados (Art. 14, IV, c):

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.

16. Relação entre a Demanda Prevista e a Contratada (Art. 14, IV, d):

Assegurar a salva guarda de dados e informações armazenadas nos servidores deste Regional, bem assim alta disponibilidade de sistemas e serviços informatizados.

Devido a restrições orçamentárias e tendência natural de aumento da quantidade de ativos de TIC na rede interna do Tribunal optamos pela modalidade de Registro de preços.

17. Adequação do Ambiente (Art. 14, V, a, b, c, d, e, f):

Não se aplica por se tratar solução abseada em appliance virtual.

18. Orçamento Estimado (Art. 14, II, g):

Conforme desclinado no Item 11

19. Sustentação do Contrato (Art.15)

19.1. Recursos Materiais e Humanos (Art. 15, I):

Não será necessária a disponibilização de recursos humanos e/ou materiais adicionais para sustentação da solução adquirida, após sua implantação.

19.2. Descontinuidade do Fornecimento (Art. 15, II):

Não se trata de um serviço de natureza contínua, logo não se aplica, smj.

19.3. Transição Contratual (Art. 15, III, a, b, c, d, e):

Não se aplica, smj, por se tratar de nova contratação/aquisição.

19.4. Estratégia de Independência Tecnológica (Art. 15, IV, a, b):

Não se trata de um serviço de natureza contínua, logo não se aplica, smj.

20. Estratégia para Contratação (Art.16)

20.1. Natureza do Objeto (Art. 16, I):

O objeto possui características comuns e usuais encontrados no mercado de TIC e trata-se de contrato de fornecimento de prorrogação de licenciamento de software com serviço de suporte e atualização, não consistindo de serviço continuado.

20.2. Parcelamento do Objeto (Art. 16, II):

Como se trata de RP é natural se pensar em parcelamento. Todavia, cada demanda, ou seja, cada ordem de fornecimento derivada do RP deverá ser realizada de maneira integral.

20.3. Adjudicação do Objeto (Art. 16, III):

Adjudicação por Lote devido a necessidade de compatibilidade e vinculos diretos entre seus itens componentes.

20.4. Modalidade e Tipo de Licitação (Art. 16, IV):

Pregão Eletrônico do Tipo Menor Preço.

20.5. Classificação e Indicação Orçamentária (Art. 16, V):

Plano de Contratação de TIC/2020

Item 11

Proposta orçamentária de 2020
Manutenção corretiva/adaptativa e sustentação de softwares
Código de classificação da fonte de recurso: 3390.40.07

20.6. Vigência da Prestação de Serviço (Art. 16, VI)

Neste caso é de 36 meses, considerando o período de garantia/suporte das licenças.

20.7. Equipe de Apoio à Contratação (Art. 16, VII):

Integrante Demandante:

Cargo ou Função: Coordenador de Infraestrutura

E-mail: coinf@tre-al.jus.br

Integrante Técnico:

Cargo ou Função: Chefe da Seção de Gerência de Infraestrutura

E-mail: segi@tre-al.jus.br

Integrante Administrativo:

Servidor: Rodrigo Ferreira Moura

E-mail: rodrigomoura@tre-al.jus.br

20.8. Equipe de Gestão da Contratação (Art. 16, VIII):

Gestor do Contrato: Indicação a cargo da Secretaria de Administração

21. Análise de Riscos:

A análise em questão é mínima, portanto, não exaustiva e focada em aspectos diretamente ligados ao procedimento nas suas etapas de aquisição e fornecimento.

Risco: 1	Não Aprovação dos documentos do Planejamento da Contratação	
Dano(s)	Atraso no processo de contratação	
Impacto(s)	Aumento de risco de vulnerabilidade exploráveis em servidores e serviços	
Ações	Responsável	Prazo
Adotar procedimentos para que a área administrativa acompanhe a elaboração dos documentos, evitando envios e devoluções do processo	Equipe de planejamento da contratação	Durante todo o processo de contratação
Reuniões com superiores para sensibilização e aprovação dos documentos.		

Risco: 2	Insuficiência de recursos orçamentários/financeiros para aquisição	
Dano(s)	Impossibilidade da contratação	
Impacto(s)	Aumento de risco de vulnerabilidade exploráveis em servidores e serviços	
Ações	Responsável	Prazo
Encontrar a maneira mais vantajosa economicamente para realizar a contratação	Equipe de planejamento da contratação	Durante todo o processo de contratação
Utilização de recursos destinados a outras aquisições para contemplar esta necessidade	STI	
Substituição dos equipamentos por outros equipamentos existentes, paralisando o andamento de outros projetos e demandas, tais como implementação de ambiente de banco de homologação e desenvolvimento.	STI	
Remanejar verbas de outros projetos previstos no plano de contratações mas que não serão executados por razões diversas	SAD	

Risco: 3	Atraso na Aquisição	
Dano(s)	Aumento de riscos na área de segurança da informação	
Impacto(s)	Eventual aumento de risco de vulnerabilidades exploráveis em servidores e serviços	
Ações	Responsável	Prazo
Solicitação de aceleração de trâmites internos	STI	Durante todo o processo de contratação
Substituição dos equipamentos por outros equipamentos existentes, paralisando o andamento de outros projetos e demandas, tais como implementação de ambiente de banco de homologação e desenvolvimento.	STI	

Risco: 4	Falha na prestação de serviços	
Dano(s)	Aumento de risco de vulnerabilidade exploráveis em servidores e serviços	
Impacto(s)	Eventual aumento de risco de vulnerabilidades exploráveis em servidores e serviços	
Ações	Responsável	Prazo
Aplicar sanções administrativas	Gestão contratual	Durante a execução do contrato
Substituição dos equipamentos por outros equipamentos existentes, caso possível, paralisando o andamento de outros projetos e demandas, tais como implementação de ambiente de banco de homologação e desenvolvimento.	STI	

A seguir se encontra a matriz de avaliação qualitativa dos riscos identificados:

Probabilidade / Impacto	Sem Impacto	Baixo	Médio	Alto
Baixa			Risco 1	
Média				Risco 2,3 e 4

Alta				

Lista de Potenciais Fornecedores

Nome: Netconn
Sítio: http://www.netconn.com.br
Telefone: (11) 3023 1500 / Ramal 5210
E-mail: comercial@netconn.com.br
Contato: Viviane Lopes

Nome: G3 Solutions
Sítio: http://www.g3solutions.com.br/
Telefone: 81 3471-8600 / 81 8173-7134
E-mail: alexandre.barros@g3solutions.com.br
Contato: Alexandre Barros

Nome: Servix
Sítio: http://www.servix.com
Telefone: (61) 3031-2960
E-mail: cristina.carvalho@servix.com
Contato: Cristina Carvalho

Nome: Service IT Security
Telefone: (11) 2595-1400
Sítio: http://www.service.com.br

Nome: SUPORTE INFORMÁTICA
Sítio: http://www.suporteinformatica.com
Telefone: 81 3202-9100 / 81 3244-9697 / 81 8178-6653
E-mail: andre.brasileiro@suporteinformatica.com
Contato: André Brasileiro

Nome: INFINIIT
Sítio: http://www.infiniit.com.br
E-mail: guilherme@infiniit.com.br
Contato: Guilherme

Nome: SWT
Sítio: http://www.swt.com.br/
Contato: Bernadete Sabino
Email: bsabino@swt.com.br
Telefone: 32213731

Nome: Plugnet
Sítio: http://www.plugnetshop.com.br/
Telefone: (81) 34267006
Contato: Breno
Email: breno@plugnetshop.com.br

Nome: PCT Informática
Sítio: http://www.pctinformatica.com.br/
Telefone: (82) 3241-5300
Contato: Zacarias
Email: pct@pctinformatica.com.br

Nome: 3A Tecnologia
Sítio: www.3atecnologia.com.br

Nome: Drive A
Sítio: www.drivea.com.br

Maceió, 04 de outubro de 2020.

Documento assinado eletronicamente por **DANIEL MACÊDO DE CARVALHO SOUTO**, **Membro da Comissão**, em 08/10/2020, às 18:11, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **CRISTINO HERMANO DE BULHÕES**, **Membro da Comissão**, em 08/10/2020, às 18:13, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **RODRIGO FERREIRA MOURA**, **Técnico Judiciário**, em 13/10/2020, às 23:36, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://sei.tre-al.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0778219** e o código CRC **6278CAE5**.

0007757-43.2020.6.02.8000 0778219v53

TRIBUNAL REGIONAL ELEITORAL DE MINAS GERAIS

AV. PRUDENTE DE MORAIS, 320 - Bairro CIDADE JARDIM - CEP 30380000 - Belo Horizonte - MG

ESTUDOS TÉCNICOS PRELIMINARES

ESTUDOS TÉCNICOS PRELIMINARES

SUMÁRIO

ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO

1. CARACTERIZAÇÃO DA DEMANDA[G1]

1.1. DESCRIÇÃO SUCINTA

Aquisição de software de gerenciamento de vulnerabilidades e análise dinâmica de aplicações web baseado em gerenciamento e armazenamento na rede local do tribunal, com licença perpetua e suporte de 36 meses.

1.2. JUSTIFICATIVA DA NECESSIDADE E RESULTADOS

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.

Por se tratar de aquisição de licença de software, não se aplicam critérios de sustentabilidade na presente contratação.

2. ESPECIFICAÇÃO DOS REQUISITOS[G2]

2.1. REQUISITOS DE NEGÓCIO[g3]

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

Regional Eleitoral de Minas Gerais.

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;

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;

Necessidade: Emissões de Relatórios;

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

2.2. REQUISITOS TECNOLÓGICOS[g4]

1. A solução deve estar licenciada e inclusa 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 500 IPs e 20 aplicações WEB;
2. A solução deve possuir recurso de varredura ativa, onde o scanner comunica-se com os alvos (ativos) através da rede;
3. A solução de gestão de vulnerabilidades deve suportar varreduras de dispositivos de IoT;
4. Deve ser capaz de identificar no mínimo 50.000 CVEs (Common Vulnerabilities and Exposures);
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;
6. Deve atribuir a todas as vulnerabilidades uma severidade baseada no CVSSv3 score;
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;
8. A solução deve fornecer criptografia de ponta a ponta dos dados de vulnerabilidades;
9. A solução deve possuir a capacidade de armazenar informações dos ativos descobertos no ambiente;
10. Deve possuir um sistema de busca de informações de um determinado ativo com no mínimo as seguintes características:
    - Por sistema operacional;
    - Por um determinado software instalado;
    - Por Ativos impactados por uma determinada vulnerabilidade.
11. A solução deve possuir suporte para a adição de detecções personalizadas usando o OVAL (Open Vulnerability Assessment Language);
12. Deve permitir aceitar o risco de uma determinada vulnerabilidade encontrada no ambiente;
13. Possibilitar alterar a criticidade de determinada vulnerabilidade de forma manual;
14. A solução deve possuir um sistema de pontuação e priorização das vulnerabilidades;
15. A solução deve ser capaz de aplicar algoritmos de aprendizagem de máquina (machine learning) para analisar as características relacionadas a vulnerabilidades;
16. O sistema de pontuação e priorização de vulnerabilidades deve avaliar no mínimo as seguintes características:
    - CVSSv3 Impact Score;
    - Idade da Vulnerabilidade;
    - Se existe ameaça ou exploit que explore a vulnerabilidade;
    - Número de produtos afetados pela vulnerabilidade;
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;
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;
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;
20. A solução deve permitir a instalação de agentes em estações de trabalho e servidores, para varredura diretamente no sistema operacional;
21. A solução deve possuir conectores para, no mínimo, as seguintes plataformas:
    - Amazon Web Service (AWS);
    - Microsoft Azure;
    - Google Clound Platform.
22. A solução deve ser capaz de produzir relatórios nos seguintes formatos: PDF, CSV, HTML e no formato de texto que poderá ser DOCX ou RTF;
23. A solução deve possuir recurso de monitoria passiva do tráfego de rede para identificação de anomalias, novos dispositivos e desvios de padrões observados;
24. A solução deve ser licenciada para o uso ilimitado de sensores passivos de rede para realizar o monitoramento em tempo real;
25. A solução deve possuir sensores, no mínimo, com as seguintes funcionalidades:
    - Execução de verificação completa do sistema (rede), adequada para qualquer host;
    - Verificação sem recomendações da rede, para que se possa personalizar totalmente as configurações da verificação;
    - Autenticação de hosts e enumeração de atualizações ausentes;
    - Execução de varredura simples para descobrir hosts ativos e portas abertas;
    - Utilização de um scanner para verificar aplicativos da web;
    - Avaliação de dispositivos móveis
    - Auditoria de configuração de serviços em nuvem de terceiros;
    - Auditoria de configuração dos gerenciadores de dispositivos móveis;
    - Auditoria de configuração dos dispositivos de rede;
    - Auditoria de configurações do sistema em relação a uma linha de base conhecida;
    - Detecção de desvio de segurança Intel AMT;
    - Verificação de malware nos sistemas Windows e Unix;
26. Deve ser possível determinar em tempo real quais portas de serviços (UDP/TCP) estão abertas em determinado ativo;
27. A solução deve ser capaz de realizar em tempo real a descoberta de novos ativos para no minímo:

- Bancos de dados;
- Hypervisors (no mímino VMWare ESX/ESXi);
- Dispositivos móveis;
- Dispositivos de rede;
- Endpoints;
- Aplicações;

28. A solução deve ser capaz de em tempo real detectar logins e downloads de arquivos em um compartilhamento de rede;
29. Permitir identificar vulnerabilidades associadas a servidores SQL no tráfego de rede;
30. A solução deve possuir interface para integração com as principais soluções de SIEM de mercado, tais como IBM QRadar, Microfocus ArcSight e Splunk.
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.
32. A atualização das ameaças deve ocorrer diariamente e sem interrupção dos serviços.
33. Configuração de segurança e acesso à gerência da solução:
    - Todos os dados armazenados nos servidores da solução devem ser criptografados e possuir logs de acesso;
    - Os dados em trânsito devem usar ao menos o algoritmo TLS 1.2 de chave 2048 bits;
    - Os dados em trânsito devem ser criptografados ao menos com o algoritmo AES-128 bits;
    - Os algoritmos de hash devem usar ao menos o algoritmo SHA-256;
    - Será aceito como comprovação critérios de criptografia, publicação em site do fabricante ou declaração do próprio fabricante;
    - Os dados armazenados devem ser criptografados ao menos com o algoritmo AES-256 bits;
    - Somente servidores da Contratante ou pessoa por ela autorizada poderão ter acesso aos dados da solução;
    - A solução deve permitir a criação de, no mínimo, 20 contas para gerência e acesso aos relatórios, sem custo adicional;
    - 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).
34. Todas as licenças de uso de software devem ser registradas, na data da entrega, em nome da Contratante no site do fabricante.
35. Dos Relatórios:
    - Deve ser capaz de executar relatórios periódicos de acordo com a frequência estabelecida pelo administrador, bem como a geração de relatórios sob demanda;
    - A solução deve possibilitar a criação de relatórios baseados na seleção de ativos, permitindo inclusive a seleção de todos os ativos existentes;
    - Deve suportar a criação de relatórios criptografados (protegidos por senha configurável);
    - A solução deve suportar o envio automático de relatórios para destinatários específicos;
    - Deve ser possível definir a frequência na geração dos relatórios para no mínimo: Diário, Mensal, Semanal e Anual;
    - Permitir especificar níveis de permissão nos relatórios para usuários e grupos específicos;
    - A solução deve fornecer relatórios do tipo “scorecard” para as partes interessadas da empresa;
    - A solução deve fornecer relatórios de correções aplicadas, classificados pelos seguintes critérios: grupo de ativos, usuários e vulnerabilidades;
36. A solução deve permitir mecanismo de varredura baseado em inferência com técnicas de varredura não intrusivas;
37. A solução deve possuir ou permitir a criação de relatórios com as seguintes informações:
    - Hosts verificados sem credenciais;
    - Top 100 Vulnerabilidades mais criticas;
    - Top 10 Hosts infectados por Malwares;
    - Hosts exploráveis por Malwares;
    - Total de vulnerabilidades que podem ser exploradas pelo Metasploit;
    - Vulnerabilidades críticas e exploráveis;
    - Máquinas com vulnerabilidades que podem ser exploradas;
38. A solução deve possuir dashboards customizáveis onde o administrador pode criar, editar ou remover painéis de acordo com a necessidade;
39. A solução deve ser capaz de inventariar todos os ativos da rede local e publicados na Internet, sem limites de endereços IPs.
40. A plataforma de software deve ser capaz de realizar varreduras (scans) de vulnerabilidades para no mínimo 500 IPs;
41. A plataforma de software deve ser licenciada para um número ilimitado de scanners (prevendo redundância);
42. Deve permitir a configuração de vários painéis e widgets;
43. Deve ser capaz de medir e reportar ameaças;
44. Deve ser capaz de visualizar ameaças críticas ao ambiente monitorado;
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;
46. A plataforma de software deve suportar vários mecanismos de varredura distribuídos em diferentes localidades e regiões e gerenciar todos por uma console central;
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;
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.
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.
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;
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;
52. A plataforma de software deve ser configurável para permitir a otimização das parametrizações de varredura;
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;
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;
55. A plataforma de software deve ser capaz de realizar pesquisas de dados confidenciais.
56. A solução deve possuir módulo para realizar varreduras de vulnerabilidades para no mínimo 20 aplicações Web, cobrindo no mínimo, mas não limitando-se a base de ameaças apontadas pelo OWASP Top 10, CWE e WASC;

- 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;
- A solução de análise deve ser capaz de analisar, testar e reportar falhas de segurança em aplicações Web;
- A solução de análise deverá ser capaz de executar varreduras em sistemas Web através de seus endereços IP ou FQDN (DNS);
- A solução de análise deve ser capaz de identificar vulnerabilidades de divulgação de dados, como vazamento de informações de identificação pessoal;
- 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;
- Deverá também permitir a execução da função crawler, que consiste na navegação para descoberta das URLs existentes na aplicação;
- A solução de análise deve suportar a integração com o softwares de automação de testes para permitir sequências de autenticação complexas;
- A solução de análise deve ser capaz de realizar testes/varreduras em aplicações separadas, simultaneamente limitadas ao número de licenças;
- Suporte a ferramentas para construção de requisições e análise de respostas de aplicações WEB, API's e WebServices, tais como Postman Collections;
- A solução de análise deve oferecer suporte à capacidade de testar novamente a vulnerabilidade específica que foi detectada anteriormente no aplicativo Web;
- Deve ser capaz de utilizar scripts customizados de crawling com parâmetros definidos pelo usuário;
- Deve ser capaz de excluir determinadas URLs da varredura através de expressões regulares;
- Deve ser capaz de excluir determinados tipos de arquivos através de suas extensões;
- 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;
- Deve ser capaz de agendar a varredura e determinar sua frequência entre uma única vez, diária, semanal, mensal e anual;
- Deve suportar o envio de notificações por email;
- Deverá ser compatível com avaliação de web services REST e SOAP;
- A solução de análise deve suportar os seguintes esquemas de autenticação:
  a. Autenticação Básica (Digest);
  b. NTLM;
  c. Autenticação de Cookies;
- Deve ser capaz de importar scripts de autenticação previamente configurados pelo usuário;
- 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;
- Os resultados devem ser apresentados agregados por vulnerabilidades ou por aplicações;
- Para cada vulnerabilidade encontrada, deve ser exibido detalhes e evidências;
- Cada vulnerabilidade encontrada deve conter também soluções propostas para mitigação ou remediação;
- 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.
- 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;
  x. Redmine

3. **AVALIAR SOLUÇÕES[G5]**

3.1. **IDENTIFICAÇÃO DAS SOLUÇÕES ADERENTES AOS REQUISITOS[a6]**

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

1. Utilização de 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.
2. Solução paga com gerenciamento e armazenamento na nuvem (On Cloud)
   - **Nome da Solução:** Ferramenta de Gestão de Vulnerabilidades On Cloud
   - **Fornecedores:** Qualys (Documento 0916613), Rapid7 (Documento 0916619) e Tenable (Documento 0916627)
   - **Descrição:** Aquisição de software de gerenciamento de vulnerabilidades e análise dinâmica de aplicações web baseado em nuvem, com modelo de subscrição por 36 meses.
3. Soluções pagas de Gestão de Vulnerabilidades On premises
   - **Fornecedores:** Rapid7 (Documento 0916619) e Tenable (Documento 0916627)
   - **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 36 meses ou de licença perpetua com suporte de 36 meses.

3.2. **COMPARAÇÃO DAS SOLUÇÕES[g7]**

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	Qte Prevista	Valor Unitário	Valor por mês	Valor Total
1	**Comunidades**	**Softwares livres OpenVas e Nmap**	**0**	**R$ -**		**R$ -**
2.1.1	Qualys (on cloud)	Licenciamento de plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando no mínimo 500 endereços IP, por 36 meses de uso e suporte do fabricante.	1	R$ 263.946,00	R$ 7.331,83	R$ 263.946,00
2.1.2	Qualys (on cloud)	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	R$ 456.840,00	R$ 7.614,00	R$ 456.840,00
2.1.3	Qualys (on cloud)	Licenciamento para solução de análise dinâmica em aplicações Web, pacote para no mínimo 10 domínios (FQDN), por 36 meses de uso e suporte do fabricante.	2	R$ 85.714,00	R$ 4.761,89	R$ 171.428,00
2.1.4	Qualys (on cloud)	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.	2	R$ 131.686,00	R$ 4.389,53	R$ 263.372,00
2.1.5	Qualys (on cloud)	Instalação e configuração.	1	R$ 6.890,00	N/A	R$ 6.890,00
2.1.6	Qualys (on cloud)	Repasse Tecnológico com período mínimo de 20 horas.	1	R$ 4.500,00	N/A	R$ 4.500,00
2.1.7	Qualys (on cloud)	4 Horas de Serviço Especializado.	10	R$ 1.250,00	N/A	R$ 12.500,00
2.1	**TOTAL Qualys (on cloud) por 36 meses**					**R$ 459.264,00**

	TOTAL Qualys (on cloud) por 60 meses					**R$ 744.102,00**
2.2.1	Rapid7 (on cloud)	Licenciamento de plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando no mínimo 500 endereços IP, por 36 meses de uso e suporte do fabricante.	1	R$ 274.025,00	R$ 7.611,81	R$ 274.025,00
2.2.2	Rapid7 (on cloud)	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	R$ 454.825,00	R$ 7.580,42	R$ 454.825,00
2.2.3	Rapid7 (on cloud)	Licenciamento para solução de análise dinâmica em aplicações Web, pacote para no mínimo 10 domínios (FQDN), por 36 meses de uso e suporte do fabricante.	2	R$ 493.245,00	R$27.402,50	R$ 986.490,00
2.2.4	Rapid7 (on cloud)	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.	2	R$ 822.075,00	R$27.402,50	R$ 1.644.150,00
2.2.5	Rapid7 (on cloud)	Instalação e configuração e repasse Tecnológico com período mínimo de 20 horas.	1	R$ 38.000,00	N/A	R$ 38.000,00
2.2.6	Rapid7 (on cloud)	Repasse Tecnológico com período mínimo de 20 horas.	1	R$ 10.000,00	N/A	R$ 10.000,00
2.2.7	Rapid7 (on cloud)	4 Horas de Serviço Especializado.	10	R$ 1.000,00	N/A	R$ 10.000,00
2.2	**TOTAL Rapid7 (on cloud) por 36 meses**					**R$ 1.318.515,00**
	TOTAL Rapid7 (on cloud) por 60 meses					**R$ 2.156.975,00**
2.3.1	Tenable (on cloud)	Licenciamento de plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando no mínimo 500 endereços IP, por 36 meses de uso e suporte do fabricante	1	R$ 316.494,00	R$ 8.791,50	R$ 316.494,00
2.3.2	Tenable (on cloud)	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	R$ 527.484,00	R$ 8.791,40	R$ 527.484,00
2.3.3	Tenable (on cloud)	Licenciamento para solução de análise dinâmica em aplicações Web, pacote para no mínimo 10 domínios (FQDN), por 36 meses de uso e suporte do fabricante.	2	R$ 115.254,00	R$ 6.403,00	R$ 230.508,00

2.3.4	Tenable (on cloud)	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.	2	R$ 192.090,00	R$ 6.403,00	R$ 384.180,00
2.3.5	Tenable (on cloud)	Instalação e configuração e repasse Tecnológico com período mínimo de 20 horas.	1	R$ 11.322,00	N/A	R$ 11.322,00
2.3.6	Tenable (on cloud)	Repasse Tecnológico com período mínimo de 20 horas	1	R$ 8.342,00	N/A	R$ 8.342,00
2.3.7	Tenable (on cloud)	4 Horas de Serviço Especializado.	10	R$ -	N/A	R$ -
2.3	**TOTAL Tenable (on cloud) por 36 meses**					**R$ 566.666,00**
	TOTAL Tenable (on cloud) por 60 meses					**R$ 931.328,00**
3.1.1	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 36 meses de uso e suporte do fabricante.	1	R$ 274.025,00	R$ 7.611,81	R$ 274.025,00
3.1.2	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	R$ 454.825,00	R$ 7.580,42	R$ 454.825,00
3.1.3	Rapid7 (on premise)	Licenciamento para solução de análise dinâmica em aplicações Web, pacote para no mínimo 10 domínios (FQDN), por 36 meses de uso e suporte do fabricante.	2	R$ 739.857,50	R$41.103,19	R$ 1.479.715,00
3.1.4	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.	2	R$ 1.233.112,50	R$41.103,75	R$ 2.466.225,00
3.1.5	Rapid7 (on premise)	Instalação e configuração e repasse Tecnológico com período mínimo de 20 horas.	1	R$ 38.000,00		R$ 38.000,00
3.1.6	Rapid7 (on premise)	Repasse Tecnológico com período mínimo de 20 horas.	1	R$ 10.000,00		R$ 10.000,00
3.1.7	Rapid7 (on premise)	4 Horas de Serviço Especializado.	10	R$ 1.000,00		R$ 10.000,00
3.1	**TOTAL Rapid7 (on premise) por 36 meses**					**R$ 1.811.740,00**
	TOTAL Rapid7 (on premise) por 60 meses					**R$ 2.979.050,00**
3.2.1	Tenable (on premise)	Licenciamento de plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando no mínimo	1	R$ 162.556,88	R$ 4.515,47	R$ 162.556,88

		500 endereços IP, por 36 meses de uso e suporte do fabricante.				
3.2.2	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	R$ 213.890,63	R$ 3.564,84	R$ 213.890,63
3.2.3	Tenable (on premise)	Licenciamento para solução de análise dinâmica em aplicações Web, pacote para no mínimo 10 domínios (FQDN), por 36 meses de uso e suporte do fabricante.	2	R$ -	R$ -	R$ -
3.2.4	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.	2	R$ -	R$ -	R$ -
3.2.5	Tenable (on premise)	Instalação e configuração.	1	R$ 11.322,00		R$ 11.322,00
3.2.6	Tenable (on premise)	Repasse Tecnológico com período mínimo de 20 horas	1	R$ 8.342,00		R$ 8.342,00
3.2.7	Tenable (on premise)	4 Horas de Serviço Especializado.	10	R$ -		R$ -
3.2	**Tenable (on premise) por 36 meses**					**R$ 182.220,88**
	Tenable (on premise) por 60 meses					**R$ 233.554,63**

4. **ESCOLHA DA SOLUÇÃO[G8]**

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.

O armazenamento de dados sensíveis em nuvem é ainda desaconselhado pela Norma Complementar 14 do Gabinete de Segurança Institucional da Presidência da República:

5.2.2 Informação sigilosa: como regra geral, deve ser evitado o tratamento em ambiente de computação em nuvem, conforme disposições a seguir:

5.2.2.1. Informação classificada: é vedado o tratamento em ambiente de computação em nuvem;

5.2.2.2. Conhecimento e informação contida em material de acesso restrito: é vedado o tratamento em ambiente de computação em nuvem;

....

5.3 Deve ser assegurado que dados, metadados, informações e conhecimento, produzidos ou custodiados por órgão ou entidade da APF, bem como suas cópias de segurança, residam em território brasileiro;

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.

Com relação ao decreto 7.174/2010 de dá preferência às soluções nacionais, informamos que não temos conhecimento de softwares nacionais com as características do objeto.

Considerando o tempo de contrato da solução, avaliamos a possibilidade de contratação pelo prazo de 36 ou 60 meses evitando os custos operacionais de realizar a mesma contratação anualmente. Acreditamos que a contratação por 36 meses caberá dentro do orçamento para a demanda. A opção de contrato por 60 meses, apesar de mais vantajosa, provavelmente extrapolaria o valor de orçamento para a aquisição.

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.

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 36 meses ou de licença perpetua com suporte de 36 meses.

Valor Estimado (baseado na melhor proposta da Tenable on premise): R$ 182.220,88 (cento e oitenta e dois mil, duzentos e vinte reais e oitenta e oito centavos).

5. **INDICAÇÃO DA NECESSIDADE DE ADEQUAÇÃO AMBIENTAL[G9]**

- Para instalação do software objeto dessa contratação no ambiente do TRE-MG, será usado o ambiente de virtualização já existente no Tribunal. Portanto já existem a infraestrutura elétrica e tecnológica e não há necessidade de mobiliário ou espaço físico.
- Será necessária mobilização da equipe de infraestrutura e alocação de servidor virtual para instalação da solução.

ANÁLISE DE SUSTENTAÇÃO DO CONTRATO

6. **RECURSOS MATERIAIS E HUMANOS[A10]**

O TRE-MG dispõe dos recursos materiais e humanos necessários à implantação e continuidade da solução.

7. **DEFINIR ATIVIDADES DE TRANSIÇÃO E ENCERRAMENTO DO CONTRATO[G11]**

Ao encerramento do contrato a licença do software deve permitir a continuidade de seu funcionamento, mesmo que não seja possível novas atualizações do software e de sua base de vulnerabilidades. Dessa forma, a renovação do contrato de suporte é interessante ao final do contrato, mas não impedirá o uso da ferramenta.

Não cabe, portanto, atividades de transição e encerramento do contrato.

8. **ELABORAR ESTRATÉGIA DE INDEPENDÊNCIA[G12]**

Considerando que a solução a ser adquirida será de propriedade do Tribunal e que será feito treinamento para sua instalação e operacionalização, não existirá dependência da fornecedora ou fabricante, exceto no que ser refere ao contrato de suporte para atualização da ferramenta.

9. **ANÁLISE DE RISCOS**

O mapa de riscos da contratação está apresentado no documento 0916610.

Assinaturas da Equipe de Planejamento da Contratação	
Mozart Fernandes Moreira Lima (NSINF) **Integrante Técnico e Demandante (Suplente)**	Gustavo Oliveira Heitmann (SANAC) **Integrante Administrativo**
Luiz Gustavo Marques Florindo (NSINF)	

Integrante Técnico e Demandante (Titular)
Data: 11/09/2020

[g1]Inserir informações baseadas no Documento de Oficialização da Demanda (DOD), que incluam a descrição sucinta da STIC pretendida, bem como a justificativa da necessida

[g2]Definir requisitos de negócio, de capacitação, legais, de manutenção, temporais, de segurança, sociais, ambientais e culturais. Além disso, especificar, quando aplicáveis, os requisitos tecnológicos com base nos requisitos anteriores.

[g3]Definir requisitos de negócio, de capacitação, legais , de manutenção, temporais, de segurança da informação, sociais, ambientais e culturais.

[g4]Especificar requisitos tecnológicos (de arquitetura tecnológica; do projeto de implantação da STIC; de garantia e manutenção; de capacitação; de experiência profissional e de formação da equipe que projetará, implantará e manterá a STIC, de metodologia de trabalho, e de segurança).

[g5]Avaliar diferentes soluções que atendam aos requisitos especificados no item anterior

[a6]Identificar as soluções aderentes aos requisitos funcionais e tecnológicos definidos, considerando:

a. Solução similar que possa ser disponibilizada por outro órgão ou entidade da APF
b. Solução similar existente no "Portal do *Software* Público Brasileiro"

Solução de mercado, verificando, inclusive, a existência de *software* livre ou *software* público

[g7]Comparar as Soluções Aderentes aos Requisitos Funcionais e Tecnológicos Definidos, considerando:

a. Estimativa do orçamento
b. Possíveis fornecedores
c. Aderência da STIC às políticas, premissas e especificações técnicas do MNI; regulamentações da ICP-Brasil e orientações do Moreq-Jus.

[g8]Escolher e justificar a solução mais adequada, abrangendo:

a. A Descrição da STIC
b. A Aderência aos Requisitos
c. A Motivação da Escolha (justificativa), indicando os resultados (objetivos) a serem alcançados.
d. A Relação entre a Demanda prevista e a STIC proposta

[g9] Avaliar as necessidades de adequação do ambiente para execução contratual, devendo abranger, no mínimo:

a) infraestrutura tecnológica;

b) infraestrutura elétrica;

c) logística de implantação;

d) espaço físico;

e) mobiliário;

f) impacto ambiental.

[a10]Identificar os recursos materiais e humanos necessários à implantação e à continuidade da solução contratada, avaliando os processos de trabalho, as normas, as políticas e as diretrizes do órgão, objetivando garantir a continuidade do negócio, inclusive após o enceramento do contrato.

[g11]Estabelecer procedimentos que devem ser seguidos em uma eventual transição contratual e no encerramento do contrato, abrangendo, no mínimo:

a) A entrega de versões finais dos produtos e da documentação, pela contratada;

b) A transferência final de conhecimentos sobre a execução e a manutenção da STIC, pela contratada;

c) A devolução/recolhimento dos recursos pela contratada ou pela contratante;

d) A revogação dos perfis de acesso, pela contratante; e

e) A eliminação de caixas postais, pela contratante.

[g12]Estabelecer diretrizes que minimizem a dependência do CONTRATANTE em relação à CONTRATADA, contemplando, quando cabíveis:

ANEXO A[A1]

Lista de Potenciais Fornecedores

	Fornecedor
1	Nome: Service IT Sítio: https://www.service.com.br/ Telefone: (11)2595-1400 E-mail: Contato: Daniel Alves e Jonata Frohlich
2	Nome: Netconn Sítio: https://www.netconn.com.br/ Telefone: (11)3023-1500 / (11)98199-7299 E-mail: Contato: Viviane Lopes
3	Nome: Servix Sítio: http://servix.com/ Telefone: (61)3031-2960 / (61)9 8144-2120 E-mail: cristina.carvalho@servix.com Contato: Cristina Carvalho

ANEXO B

- Pregão Eletrônico Nº 6/2017 – Ministério da Economia - Aquisição de Licença e Garantia de Software de Solução de Gestão de Vulnerabilidades e Conformidade pelo período de 48 meses; Contratação de Serviço Especializado, pelo período de 48 meses, em Gestão de Vulnerabilidades e Conformidade em Ativos e Sistemas de TIC; e em Análise de Vulnerabilidades em Sistemas de TIC. Contratação de Banco de Horas, pelo período de 48 meses, para a realização de Testes de Invasão nos Ativos e Sistemas de TIC do Banco Central do Brasil (Bacen). As demais características são aquelas descritas no Anexo 1 do Edital de Pregão Eletrônico.

- Pregão Eletrônico Nº 12/2018 – Cia. de Processamento de Dados do Estado de São Paulo - Prestação de Serviços e licenciamento de uso de software de sistema integrado de gerenciamento de vulnerabilidades para aplicativos web e ativos de rede, incluindo implantação, suporte técnico, garantia e manutenção de versões, treinamento especializado e operação assistida do sistema.

- Pregão Eletrônico Nº 1/2020 – Conselho da Justiça Federal - Contratação de Serviços Gerenciados de Segurança da Informação para o Conselho da Justiça Federal – CJF

    a) Serviços de Operação e Atendimento à Requisições;

    b) Serviço de Gestão de Incidentes de Segurança (CSIRT - Blue Team);

    c) Serviço de Gestão de Vulnerabilidades;

    d) Serviço de Monitoramento e Visibilidade de Ataques Cibernéticos;

    e) Serviço de Orquestração, Automação e Resposta de Segurança (SOAR);

    f) Serviço de Testes de Invasão (Red Team).

ANEXO C

O dimensionamento da solução foi feito com base em levantamento dos principais equipamentos conectados à rede do TRE-MG identificando ativos passíveis de gestão de vulnerabilidades. Os detalhes dos ativos foram omitidos por questões de segurança..

Tipo de Ativo	3com	Aruba	Brocade	Checkpoint	Cisco	Dell	D-link	EMC	Ericsson	F5	HP	Lenovo	Microsoft	Oracle	Paloalto	V
Backbone Primário																
Backbone Secundário					4											
Backup											1					
Descktop Virtual																
DMZ										3						
Firewalls Backbone Primário										3					1	
Gerência	30	26	2	2	5	19	4	2		2	11	1		1	5	
Gerência Access Point															1	
Link ADS 320					1					4						
Link Internet Prédio 100					1					3						
Link Internet Prédio 320										2						
Rede Justiça Eleitoral				1						1						
Reservado Firewall										3						
Sala Cofre															1	
Segurança (Câmeras de Vídeo)										1						
Servicores em Produção													1	1		
Servidores de Desenvolvimento																
Servidores de Teste																
Servidores em Homologação																
VoIP									4						1	
TOTAL	**30**	**26**	**2**	**3**	**11**	**19**	**4**	**2**	**4**	**22**	**12**	**1**	**1**	**2**	**9**	

Também foi considerada uma relação das principais aplicações Web do TRE-MG:

1. AcolheMinas
2. Averbacao Cursos
3. Concurso de remoção
4. Defeito urna
5. Denúncia online
6. eJusPJE
7. Fale Conosco
8. Inscrição de Eventos
9. Instrutoria
10. Juízes
11. Margem consignável
12. Mesários - confirmação da convocação
13. Ouvidoria
14. Pesquisas diversas
15. Portal de Serviços Extranet
16. Serpro GRU
17. Siel Transparência do CNJ
18. Validação de certificados

[a1]Incluir todos os anexos que se fizerem necessários.

Em de de .

Documento assinado eletronicamente por **MOZART FERNANDES MOREIRA LIMA**, **Técnico Judiciário**, em 25/09/2020, às 12:41, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **LUIZ GUSTAVO MARQUES FLORINDO**, **Analista Judiciário**, em 25/09/2020, às 18:54, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **GUSTAVO OLIVEIRA HEITMANN**, **Técnico Judiciário**, em 28/09/2020, às 15:19, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade deste documento pode ser conferida no site https://sei.tre-mg.jus.br/controlador_externo.php?acao=documento_conferir&acao_origem=documento_conferir&lang=pt_BR&id_orgao_acesso_externo=0, informando o código verificador **0966369** e o código CRC **72FEFC21**.

TRIBUNAL REGIONAL ELEITORAL DE MINAS GERAIS

AV. PRUDENTE DE MORAIS, 100 - Bairro CIDADE JARDIM - CEP 30380000 - Belo Horizonte - MG

TERMO DE REFERÊNCIA OU PROJETO BÁSICO

TERMO DE REFERÊNCIA

SUMÁRIO

1. CARACTERIZAÇÃO DO OBJETO

DEFINIÇÃO DO OBJETO[G1]

Aquisição de software de gerenciamento de vulnerabilidades e análise dinâmica de aplicações web baseado em gerenciamento e armazenamento na rede local do tribunal, com licença perpetua e suporte de 36 meses.

2. FUNDAMENTAÇÃO DA CONTRATAÇÃO

2.1. JUSTIFICATIVA DA NECESSIDADE E RESULTADOS[G2]

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.

Por se tratar de aquisição de licença de software, não se aplicam critérios de sustentabilidade na presente contratação.

2.2. ALINHAMENTO ESTRATÉGICO[G3]

Aperfeiçoamento da governança de tecnologia da informação — Busca garantir os meios que viabilizem a definição, o planejamento, a priorização e a implantação de soluções tecnológicas que apoiem os processos essenciais do TRE-MG, os controles efetivos dos processos de segurança e de riscos, assim como os serviços voltados para a sociedade, com utilização eficiente de recursos. Otimizar o uso dos recursos/ativos de TIC —

Estruturar a tecnologia da informação e o seu gerenciamento a fim de garantir o desenvolvimento, aperfeiçoamento e a disponibilidade dos sistemas essenciais à execução das atividades judiciais e administrativas. Conhecer e estabelecer um processo responsável por manter as informações sobre os itens de configuração necessários para a entrega de serviços de TIC, incluindo seus relacionamentos.

A presente contratação atende aos seguintes objetivos estratégicos do PETIC 2016-2021

- OE-02 Buscar soluções integradas que contribuam para o desenvolvimento institucional
- OE-03 Otimizar o uso dos recursos/ativos de TIC
- OE-04 Implantar as determinações estabelecidas na Política de Segurança da Informação
- OE-10 Garantir a conformidade de TIC e apoio para conformidade do negócio com as leis e regulações externas

2.3. REFERÊNCIA AOS ESTUDOS PRELIMINARES[G4]

Os estudos técnicos preliminares são apresentados no documento 0966369 deste processo administrativo.

2.4. RELAÇÃO ENTRE A DEMANDA PREVISTA E A STIC A SER CONTRATADA[G5]

Conforme anexo C do Estudo Técnico Preliminar (documento 0966369), foram levantados 496 endereços IP passíveis de monitoramento de vulnerabilidades. Considerando que parte desses endereços podem ser monitorados por amostragem (o que reduz a demanda) contrapõe à expectativa de crescimento de endereços IP na rede do TRE-MG, estimamos que o monitoramento de 500 endereços IP atenderá a demanda para os próximos 3 anos.

Ainda conforme levantado no mesmo anexo C, foram levantadas 18 aplicações Web disponíveis na Intranet e Internet do Tribunal, cabendo portanto no pacote de 20 aplicações solicitadas nesta contratação.

Devem ser adiquiridos:

- 01 (um) licenciamento de plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando no mínimo 500 endereços IP, por 36 meses de uso e suporte do fabricante;
- 02 (dois) licenciamentos para solução de análise dinâmica em aplicações Web, pacote para no mínimo 10 domínios (FQDN), por 36 meses de uso e suporte do fabricante.
- Serviços de instalação e configuração.
- Repasse Tecnológico com período mínimo de 20 horas.
- 40 Horas de Serviço Especializado para ser usado sob demanda dentro do período do contrato.

2.5. JUSTIFICATIVA DA STIC ESCOLHIDA [G6]

Considerando as soluções propostas no item 3.2 (Comparação das Soluções) do Estudo Técnico Preliminar (0966369), concluímos:

- a solução 1 mostrou-se incompleta para atender as demandas do TRE-MG;
- a solução 2 mostrou-se inadequada por armazenar dados críticos em nuvem pública, contrariando a recomendação da Norma Complementar 14 do Gabinete de Segurança Institucional da Presidência da República;
- a solução 3 mostrou-se a mais adequada em termos técnicos, de regulamentação e economicidade.

Portanto, a escolha técnica foi pela solução para gerenciamento de vulnerabilidades e analise dinâmica web baseado em gerenciamento e armazenamento na rede local do Tribunal, com licença perpétua e suporte de 36 meses.

2.6. JUSTIFICATIVA PARA A UTILIZAÇÃO DO SRP [G7]

Solicitamos adesão como partícipe à ARP (Ata de Registro de Preços) proposta pelo TRE-PB com abertura para adesão aos demais TREs. O processo está sendo tratado no SEI daquele tribunal sob o número 0008787-53.2020.6.15.8000 e registrada no portal de aquisições do TSE no site http://sticonhecimento.tse.jus.br/informes/2020/portal-de-aquisicoes-de-ti.

2.7. FORMA DE PARCELAMENTO E ADJUDICAÇÃO DO OBJETO[G8]

Solução com armazenamento e gerenciamento local (on premisse)

Item	Descrição	Quantidade
01	Licenciamento de plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando no mínimo 500 endereços IP, por 36 meses de uso e suporte do fabricante.	01
02	Licenciamento para solução de análise dinâmica em aplicações Web, pacote para no mínimo 10 domínios	02

	(FQDN), por 36 meses de uso e suporte do fabricante.	
03	Instalação e configuração.	01
04	Repasse Tecnológico com período mínimo de 20 horas	01
05	4 Horas de Serviço Especializado.	01

A solução proposta deve ser de mesmo fabricante, sem adaptações ou alterações, disponível para gerenciamento em console central unificado.

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;

A adjudicação será feita de forma completa, tendo em vista trata-se de solução não divisível e por compor solução tecnológica

2.8. **DIREITO DE PREFERÊNCIA[G9]**

Com relação ao decreto 7.174/2010 de dá preferência às soluções nacionais, informamos que não temos conhecimento de softwares nacionais com as características do objeto.

3. **ESPECIFICAÇÃO TÉCNICA[G10]**

3.1. DESCRIÇÃO DA SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO REQUISITOS DA CONTRATAÇÃO

3.1.1 Requisitos gerais da solução

3.1.1.1 A solução deve estar licenciada e inclusa 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);

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

3.1.1.3 A solução de gestão de vulnerabilidades deve suportar varreduras de dispositivos de IoT;

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

3.1.1.5 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;

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

3.1.1.7 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;

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

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

3.1.1.10 Deve possuir um sistema de busca de informações de um determinado ativo com no mínimo as seguintes características:

3.1.1.10.1 Por sistema operacional;

3.1.1.10.2 Por um determinado software instalado;

3.1.1.10.3 Por Ativos impactados por uma determinada vulnerabilidade.

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

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

3.1.1.13 Possibilitar alterar a criticidade de determinada vulnerabilidade de forma manual;

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

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

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

3.1.1.16.1 CVSSv3 Impact Score;

3.1.1.16.2 Idade da Vulnerabilidade;

3.1.1.16.3 Se existe ameaça ou exploit que explore a vulnerabilidade;

3.1.1.16.4 Número de produtos afetados pela vulnerabilidade;

3.1.1.17 Deve ser capaz de fazer a correlação em tempo real de ameaças ativas contra vulnerabilidades encontradas, incluindo feeds de inteligência de ameaças ao vivo;

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

3.1.1.19 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;

3.1.1.20 A solução deve permitir a instalação de agentes em estações de trabalho e servidores, para varredura diretamente no sistema operacional;

3.1.1.21 A solução deve ser capaz de produzir relatórios nos seguintes formatos: PDF, CSV e HTML;

3.1.1.22 A solução deve possuir recurso de monitoria passiva do tráfego de rede para identificação de anomalias, novos dispositivos e desvios de padrões observados;

3.1.1.23 A solução deve ser licenciada para o uso ilimitado de sensores passivos de rede para realizar o monitoramento em tempo real;

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

3.1.1.24.1 Execução de verificação completa do sistema (rede), adequada para qualquer host;

3.1.1.24.2 Verificação sem recomendações da rede, para que se possa personalizar totalmente as configurações da verificação;

3.1.1.24.3 Autenticação de hosts e enumeração de atualizações ausentes;

3.1.1.24.4 Execução de varredura simples para descobrir hosts ativos e portas abertas;

3.1.1.24.5 Utilização de um scanner para verificar aplicativos da web;

3.1.1.24.6 Avaliação de dispositivos móveis;

3.1.1.24.7 Auditoria de configuração de serviços em nuvem de terceiros;

3.1.1.24.8 Auditoria de configuração dos gerenciadores de dispositivos móveis;

3.1.1.24.9 Auditoria de configuração dos dispositivos de rede;

3.1.1.24.10 Auditoria de configurações do sistema em relação a uma linha de base conhecida;

3.1.1.24.11 Detecção de desvio de segurança Intel AMT (Active Management Techonology);

3.1.1.24.12 Verificação de malware nos sistemas Windows e Unix;

3.1.1.25 Deve ser possível determinar em tempo real quais portas de serviços (UDP/TCP) estão abertas em determinado ativo;

3.1.1.26 A solução deve ser capaz de realizar em tempo real a descoberta de novos ativos para no mínimo:

3.1.1.26.1 Bancos de dados;

3.1.1.26.2 Hypervisors (no mínimo VMWare ESX/ESXi);

3.1.1.26.3 Dispositivos móveis;

3.1.1.26.4 Dispositivos de rede;

3.1.1.26.5 Endpoints;

3.1.1.26.6 Aplicações;

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

3.1.1.28 Permitir identificar vulnerabilidades associadas a servidores SQL no tráfego de rede;

3.1.1.29 A solução deve possuir interface para integração com as principais soluções de SIEM de mercado, tais como IBM QRadar, Microfocus ArcSight e Splunk.

3.1.1.30 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.

3.1.1.31 A atualização das ameaças deve ocorrer diariamente e sem interrupção dos serviços.

3.1.1.32 Configuração de segurança e acesso à gerência da solução:

3.1.1.32.1 Todos os dados armazenados nos servidores da solução devem ser criptografados e possuir logs de acesso;

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

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

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

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

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

3.1.1.32.7 Somente servidores da Contratante ou pessoa por ela autorizada poderão ter acesso aos dados da solução;

3.1.1.32.8 A solução deve permitir a criação de, no mínimo, 20 contas para gerência e acesso aos relatórios, sem custo adicional;

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

3.1.1.33 Todas as licenças de uso de software devem ser registradas, na data da entrega, em nome da Contratante no site do fabricante.

3.1.1.34 A licitante deverá apresentar, juntamente à proposta ajustada ao seu último lance, **declaração ou documento da fabricante** que comprove estar autorizada a comercializar, instalar, configurar e prestar suporte das licenças objeto deste certame. Tal exigência baseia-se na intenção de evitar que uma empresa arrematante seja declarada vencedora do certame, por ter oferecido o menor valor para os licenciamentos especificados, não venha a concluir o fornecimento assumido, justamente por falta da anuência/autorização da fabricante dos produtos, que pode se negar à arrematante a fornecer produtos,

fato que levaria ao fracasso da licitação e certamente acarretaria prejuízos à este Tribunal e multas e demais penalidades à arrematante.

3.1.1.35 Dos Relatórios:

3.1.1.35.1 Deve ser capaz de executar relatórios periódicos de acordo com a frequência estabelecida pelo administrador, bem como a geração de relatórios sob demanda;

3.1.1.35.2 A solução deve possibilitar a criação de relatórios baseados na seleção de ativos, permitindo inclusive a seleção de todos os ativos existentes;

3.1.1.35.3 Deve suportar a criação de relatórios criptografados (protegidos por senha configurável);

3.1.1.35.4 A solução deve suportar o envio automático de relatórios para destinatários específicos;

3.1.1.35.5 Deve ser possível definir a frequência na geração dos relatórios para no mínimo: Diário, Mensal, Semanal e Anual;

3.1.1.35.6 Permitir especificar níveis de permissão nos relatórios para usuários e grupos específicos;

3.1.1.35.7 A solução deve fornecer relatórios do tipo “scorecard” para as partes interessadas da empresa;

3.1.1.35.8 A solução deve fornecer relatórios de correções aplicadas, classificados pelos seguintes critérios: grupo de ativos, usuários e vulnerabilidades;

3.1.1.36 A solução deve permitir mecanismo de varredura baseado em inferência com técnicas de varredura não intrusivas;

3.1.1.37 A solução deve possuir ou permitir a criação de relatórios com as seguintes informações:

3.1.1.37.1 Hosts verificados sem credenciais;

3.1.1.37.2 Top 100 Vulnerabilidades mais críticas;

3.1.1.37.3 Top 10 Hosts infectados por Malwares;

3.1.1.37.4 Hosts exploráveis por Malwares;

3.1.1.37.5 Total de vulnerabilidades que podem ser exploradas pelo Metasploit;

3.1.1.37.6 Vulnerabilidades críticas e exploráveis;

3.1.1.37.7 Máquinas com vulnerabilidades que podem ser exploradas;

3.1.1.38 A solução deve possuir dashboards customizáveis onde o administrador pode criar, editar ou remover painéis de acordo com a necessidade;

3.1.1.39 A solução deve ser capaz de inventariar todos os ativos da rede local e publicados na Internet, sem limites de endereços IPs.

3.1.1.40 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.

3.1.1.41 A 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).

3.1.1.42 A aquisição da plataforma de software de gestão de vulnerabilidades (item 01) é pré-requisito para a contratação do módulo de análise dinâmica de aplicações web (item 02).

3.1.1.43 Caso a licença da plataforma de software de gestão de vulnerabilidades (item 01) contemple a análise dinâmica de aplicações web, o licitante deverá apresentar R$ 0,00 (zero reais) como o preço dos itens relacionados a análise dinâmica de aplicações web (item 02).

3.1.1.44 A solução proposta deve ser de mesmo fabricante, sem adaptações ou alterações, disponível para gerenciamento em console central unificado.

3.1.1.45 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;

3.1.2 Características técnicas mínimas do item 01 - Licenciamento de plataforma on premisse de gestão de vulnerabilidades e auditoria de configurações de ativos de rede:

3.1.2.1 A plataforma de software deve ser capaz de realizar varreduras (scans) de vulnerabilidades, de acordo com a quantidade de endereços IP licenciados;

3.1.2.2 A plataforma de software deve ser licenciada para um número ilimitado de scanners (prevendo redundância);

3.1.2.3 Deve permitir a configuração de vários painéis e widgets;

3.1.2.4 Deve ser capaz de medir e reportar ameaças;

3.1.2.5 Deve ser capaz de visualizar ameaças críticas ao ambiente monitorado;

3.1.2.6 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;

3.1.2.7 A plataforma de software deve suportar vários mecanismos de varredura distribuídos em diferentes localidades e regiões e gerenciar todos por uma console central;

3.1.2.8 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;

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

3.1.2.10 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.

3.1.2.11 A plataforma de software deve incluir a capacidade de programar períodos em que varreduras não podem ser executadas, como por exemplo em determinados dias do mês ou determinados horários do dia;

3.1.2.12 No caso em que uma atividade de varredura seja interrompida por invadir o período não permitido, a varredura deve ser capaz de ser reiniciada de onde parou;

3.1.2.13 A plataforma de software deve ser configurável para permitir a otimização das parametrizações de varredura;

3.1.2.14 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;

3.1.2.15 A plataforma de software deve fornecer a capacidade de escalar privilégios nos destinos, do acesso de usuário padrão até acesso de sistema ou administrativo;

3.1.2.16 A plataforma de software deve ser capaz de realizar pesquisas de dados confidenciais.

3.1.3 Características técnicas mínimas do item 02 - Licenciamento para solução de análise dinâmica em aplicações Web

3.1.3.1 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;

3.1.3.2 A solução de análise deve ser capaz de analisar, testar e reportar falhas de segurança em aplicações Web;

3.1.3.3 A solução de análise deverá ser capaz de executar varreduras em sistemas Web através de seus endereços IP ou FQDN (DNS);

3.1.3.4 A solução de análise deve ser capaz de identificar vulnerabilidades de divulgação de dados, como vazamento de informações de identificação pessoal;

3.1.3.5 Para varreduras extensas e detalhadas, deve varrer e auditar no mínimo os seguintes elementos:

3.1.3.5.1 Cookies, Headers, Formulários e Links;

3.1.3.5.2 Nomes e valores de parâmetros da aplicação;

3.1.3.5.3 Elementos JSON e XML;

3.1.3.5.4 Elementos DOM;

3.1.3.6 Deverá também permitir a execução da função crawler, que consiste na navegação para descoberta das URLs existentes na aplicação;

3.1.3.7 A solução de análise deve suportar a integração com softwares de automação de testes para permitir sequências de autenticação complexas;

3.1.3.8 A solução de análise deve ser capaz de realizar testes/varreduras em aplicações separadas simultaneamente, limitadas ao número de licenças;

3.1.3.9 A solução de análise deve oferecer suporte à capacidade de testar novamente a vulnerabilidade específica que foi detectada anteriormente no aplicativo Web;

3.1.3.10 Deve ser capaz de utilizar scripts customizados de crawling com parâmetros definidos pelo usuário;

3.1.3.11 Deve ser capaz de excluir determinadas URLs da varredura através de expressões regulares;

3.1.3.12 Deve ser capaz de excluir determinados tipos de arquivos através de suas extensões;

3.1.3.13 Deve ser capaz de instituir no mínimo os seguintes limites:

3.1.3.13.1 Número máximo de URLs para crawling e navegação;

3.1.3.13.2 Número máximo de diretórios para varreduras;

3.1.3.13.3 Tamanho máximo de respostas;

3.1.3.13.4 Tempo máximo para a varredura;

3.1.3.14 Deve ser capaz de agendar a varredura e determinar sua frequência entre uma única vez, diária, semanal, mensal e anual;

3.1.3.15 Deve suportar o envio de notificações por e-mail;

3.1.3.16 Deverá ser compatível com avaliação de web services REST e SOAP;

3.1.3.17 A solução de análise deve suportar os seguintes esquemas de autenticação:

3.1.3.17.1 Autenticação Básica (Digest);

3.1.3.17.2 NTLM;

3.1.3.17.3 Autenticação de Cookies;

3.1.3.18 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;

3.1.3.19 Os resultados devem ser apresentados agregados por vulnerabilidades ou por aplicações;

3.1.3.20 Para cada vulnerabilidade encontrada, deve ser exibido detalhes e evidências;

3.1.3.21 Cada vulnerabilidade encontrada deve conter também soluções propostas para mitigação ou remediação;

3.1.3.22 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.

3.1.3.23 A solução deve ser capaz de realizar varreduras nos seguintes componentes/aplicações:

3.1.3.23.1 WordPress;

3.1.3.23.2 IIS 6.x e IIS 10.x;

3.1.3.23.3 ASP 6;

3.1.3.23.4 NET 2;

3.1.3.23.5 Apache HTTPD 2.2.x e 2.4.x;

3.1.3.23.6 Tomcat 6.x, 7.x, 8.x e superiores;

3.1.3.23.7 Jetty 8 e superiores;

3.1.3.23.8 Nginx;

3.1.3.23.9 PHP 5.3.x, 5.4.x, 5.6.x, 7.0.x e 7.1.x e superiores;

3.1.3.23.10 Java 1.5, 1.6, 1.7 e 1.8 e superiores;

3.1.3.23.11 Jboss 4.x e 7.x e superiores;

3.1.3.23.12 WildFly 8 e 10 e superiores;

3.1.3.23.13 Plone 2.5.x e 4.3.x e superiores;

3.1.3.23.14 Zope;

3.1.3.23.15 Python 2.4.4 e superiores;

3.1.3.23.16 J2EE;

3.1.3.23.17 Ansible;

3.1.3.23.18 Joomla;

3.1.3.23.19 Moodle;

3.1.3.23.20 Docker Conteiner;

3.1.3.23.21 Elk;

3.1.3.23.22 GIT;

3.1.3.23.23 Grafana; e

3.1.3.23.24 Redmine.

3.1.4 Características técnicas mínimas do item 03 – Instalação e Configuração da Solução

3.1.4.1 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;

3.1.4.2 Apoio na instalação de scanners e agentes on-premises;

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

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

3.1.4.5 Não serão aceitos softwares "beta" ou em desenvolvimento;

3.1.4.6 Somente será aceita a instalação por técnico certificado na fabricante da solução, da CONTRATADA ou do fabricante;

3.1.4.7 A CONTRATADA deverá elaborar documentação, contendo no mínimo os seguintes itens:

3.1.4.7.1 Cronograma;

3.1.4.7.2 Levantamento de informações sobre o ambiente atual;

3.1.4.7.3 Definição dos parâmetros de configuração básicos e avançados a serem implementados;

3.1.4.7.4 Mapa de rede contendo a topologia a ser implementada ou atualizada;

3.1.4.7.5 Gerenciamento de mudanças, contemplando análise de riscos de implementação da solução;

3.1.4.7.6 Procedimentos de implementação e de rollback no caso de problemas não previstos previamente.

3.1.4.8 A CONTRATADA poderá subcontratar uma empresa autorizada pelo fabricante para atender as atividades relacionadas ao Instalação e Configuração.

3.1.5 Características técnicas mínimas do item 04 – Repasse Tecnológico

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

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

3.1.5.2.1 Procedimentos de instalação física e lógica;

3.1.5.2.2 Todos os procedimentos necessários à configuração técnica;

3.1.5.2.3 Todos os procedimentos necessários à completa operação do produto; e

3.1.5.2.4 Todos os procedimentos de manutenção do produto que devem ser realizados pelos técnicos do órgão.

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

3.1.5.4 O treinamento deverá ser ministrado em horário definido pelo tribunal, em dias úteis;

3.1.5.5 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.

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

3.1.6 Características técnicas mínimas do item 05 – Serviço Especializado

3.1.6.1 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:

3.1.6.1.1 Acompanhar, quando solicitado por um usuário, todas as operações realizadas no sistema durante determinado período;

3.1.6.1.2 Esclarecer dúvidas de usuários em relação à operação do sistema;

3.1.6.1.3 Prestar serviços de suporte técnico para a solução de problemas que impeçam o perfeito funcionamento do sistema;

3.1.6.1.4 Reportar à Coordenação de informática do órgão quaisquer outros problemas verificados durante o atendimento, relativos ou não à solução fornecida;

3.1.6.1.5 Fornecer informações aos usuários sobre a situação e o andamento de serviços de manutenção solicitados;

3.1.6.1.6 Diagnosticar a performance do software em seus aspectos operacionais;

3.1.6.1.7 Identificar problemas inerentes ao software e ao ambiente onde este se encontra instalado;

3.1.6.1.8 Discutir implementações de melhorias, visando possíveis adequações;

3.1.6.1.9 Na prestação dos serviços de operação assistida, a Contratada deverá utilizar profissionais com qualificação e treinamento adequados para o desenvolvimento das tarefas relacionadas anteriormente;

3.1.6.1.10 Apoio no desenvolvimento de dashboad´s e solução de problemas internos, relativos às licenças adquiridas;

3.1.6.1.11 Integração da solução com ferramentas de ITSM;

3.1.6.1.12 Documentação e transferência de conhecimento das atividades técnicas realizadas.

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

3.1.6.3 O licitante poderá apresentar R$ 0,00 (zero reais) como o preço dos itens relacionados ao Bloco de 04 Horas de Serviço Especializado (item 05) caso os serviços elencados estejam incluídos no preço da solução ofertada da ferramenta de gestão de vulnerabilidades;

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

3.2. REQUISITOS DA SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO[S11]

3.2.1 Local onde os softwares e licenças deverão ser entregues e instalados:

Tribunal Regional Eleitoral de Minas Gerais – ANEXO 1
Av. Prudente de Morais, 320
Bairro Cidade Jardim
Belo Horizonte, MG
CEP 30380-002

3.2.2 Condições de participação e realização dos serviços

3.2.2.1 A solução será constituída de softwares, licenças e serviços relacionados nos itens especificados, sendo todos de um mesmo fabricante, garantindo a entrega e execução dos serviços por uma única empresa e a total compatibilidade entre eles;

3.2.2.2 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.

3.2.3 Garantia e Suporte Técnico

3.2.3.1 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;

3.2.3.1.1 O suporte pelo fabricante será obrigatório;

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

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

3.2.3.3 O tempo da garantia e suporte técnico será de 36 meses;

3.2.3.4 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;

3.2.3.5 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 registrado no item 03;

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

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

3.2.3.6.2 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);

3.2.3.6.3 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);

3.2.3.6.4 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);

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

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

3.2.3.9 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;

3.2.3.10 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;

3.2.3.11 Os chamados abertos por e-mail deverão ter sua abertura automática no portal web;

3.2.3.12 Todo o chamado aberto deverá ter sua resolução técnica registrada no sistema web de help-desk;

3.2.3.13 A contratante poderá solicitar o escalonamento de incidentes ao fabricante quando se tratar de correções especiais, defeitos nos programas ou defeito em hardware;

3.2.3.14 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;

3.2.3.15 A garantia iniciará sua contagem a partir da data de emissão da NF dos softwares, serviços ou licenças;

3.2.3.16 Havendo discrepâncias entre o que está especificado no item específico e o que consta nestas condições gerais, prevalecerá o que está no item específico.

3.2.4 Atualizações

3.2.4.1 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 (36 meses), sem qualquer ônus adicional para o contratante;

3.2.4.2 As atualizações incluídas devem ser do tipo "minor release" e "major release", permitindo manter todos componentes atualizados em sua última versão de software/firmware.

3.2.5 Condições de entrega e recebimento

3.2.5.1 Para os itens 01 e 02, o fornecimento das licenças de software deverá ocorrer em até 05 (cinco) dias úteis após a assinatura do contrato.

3.2.5.2 Para o item 03, 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.

3.2.5.3 Para o item 04, 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.

3.2.5.4 O item 05 - 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.

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

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

3.2.5.7 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;

3.2.5.8 Para itens de software, devem ser apresentados chave única tipo serial ou qualquer outra forma de validação da ferramenta, comprovando perante o fabricante que se trata de uma ferramenta devidamente licenciada;

3.2.5.9 O Termo de Recebimento Provisório será emitido por servidor ou comissão do TRE-MG, devidamente constituída para este fim, em até 5 dias úteis após a entrega dos itens;

3.2.5.10 O Termo de Recebimento Definitivo será emitido por servidor ou comissão do TRE-MG devidamente constituída para este fim em até 10 dias úteis após a entrega.

3.2.6 Condições de aceite

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

3.2.6.2 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. Para a amostra, a empresa deverá apresentar as mesmas verões do produto ofertado no certame, com técnico certificado na solução para configuração e comprovação dos itens pendentes, nas dependências deste órgão, conforme itens 1.1.1 e 1.1.2, TC-006.806/2006-4, Acórdão nº 838/2006-TCU-2ª Câmara.

3.3. FIXAÇÃO DAS ROTINAS DE EXECUÇÃO DO CONTRATO[G12]

3.3.1 Para os itens 01 e 02, o fornecimento das licenças de software deverá ocorrer em até 05 (cinco) dias úteis após a assinatura do contrato.

3.3.2 Para o item 03, 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.

3.3.3 Para o item 04, 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.

3.3.4 O item 05 - 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.

3.4. MODELOS DE TERMOS RELATIVOS À SEGURANÇA DA INFORMAÇÃO[G13]

A empresa contratada deverá respeitar as diretrizes constantes da Política de Segurança da Informação do TRE-MG (Resolução TRE-MG 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 de Minas Gerais aos quais tiver acesso em decorrência do objeto da presente contratação, ficando terminantemente proibida de fazer uso ou revelação destes sob qualquer justificativa;

O Tribunal Regional Eleitoral de Minas Gerais terá propriedade sobre todos os documentos e procedimentos operacionais produzidos no escopo da presente contratação;

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

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. QUALIFICAÇÃO TÉCNICA[G14]

A PROPONENTE deverá:

4.1 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;

4.2 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:

4.2.1 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.

5. ESTRATÉGIA DA CONTRATAÇÃO

5.1. VIGÊNCIA DA CONTRATAÇÃO[G15]

O contrato decorrente da contratação terá vigência de 36 meses.

5.2. DEFINIÇÃO DAS OBRIGAÇÕES DO CONTRATANTE[G16]

5.2.1 Receber provisoriamente o material, disponibilizando local, data e horário.

5.2.2 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.

5.2.3 Acompanhar e fiscalizar o cumprimento das obrigações da Contratada, através do gestor e dos fiscais especialmente designados.

5.2.4 Efetuar o pagamento na forma e no prazo previsto neste instrumento e no contrato

5.3. DEFINIÇÃO DAS OBRIGAÇÕES DO CONTRATADO[G17]

5.3.1 Fornecer todas as licenças de software necessárias para utilização completa da solução, pelos períodos adquiridos.

5.3.2 Registrar, junto aos fabricantes e em nome da contratante, todas as assinaturas de licenças de software ofertadas.

5.3.3 Cumprir fielmente as obrigações assumidas, conforme as especificações constantes neste Termo de Referência, utilizando-se de todos os recursos materiais e humanos necessários para entregar os produtos/prestar os serviços, nos prazos indicados.

5.3.4 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.

5.3.5 Prestar todos os esclarecimentos que forem solicitados pelo TRE-MG, credenciando junto ao órgão, um representante para prestar os devidos esclarecimentos e atender as reclamações que porventura surgirem durante a execução do objeto.

5.3.6 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.

5.3.7 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.

5.3.8 Executar os serviços nos prazos estabelecidos neste instrumento, nos locais indicados pela Administração, em estrita observância das especificações do Edital e da proposta;

5.3.9 Atender prontamente aos chamados da Administração, relacionados ao objeto da licitação;

5.3.10 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;

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

5.3.12 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.

5.3.13 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.

5.3.14 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.

5.4. **FORMA DE PAGAMENTO[G18]**

O pagamento será feito por etapas, ao final da conclusão de cada uma delas:

5.4.1 - Em até 10 dias úteis após licenciamento e instalação da solução, atendendo os itens 01, 02 e 03;

5.4.2 - Em até 10 dias úteis após repasse tecnológico conforme item 04;

5.4.3 - Em até 10 dias úteis após prestação do(s) bloco(s) de 4 horas de serviço técnico conforme item 05.

5.5. **FIXAÇÃO DOS CRITÉRIOS DE ACEITAÇÃO[G19]**

Para os itens 1, 2 e 3 o aceite será dado por representante do TRE-MG após validação da solução instalada e em funcionamento conforme especificado

Para o item 4, o aceite será dado por representante do TRE-MG após repasse tecnológico para até 10 servidores do Tribunal.

Para o item 5, o aceite será dado por representante do TRE-MG após atestação de horas de serviço especializado solicitadas sob demanda.

5.6. **INDICAÇÃO DOS PROCEDIMENTOS MÍNIMOS DE TESTE E INSPEÇÃO[G20]**

Não se aplica ao objeto desa contratação.

5.7. **RETENÇÕES OU GLOSAS[G21]**

Não se aplica ao objeto desa contratação.

5.8. **SANÇÕES ADMINISTRATIVAS[G22]**

Pelo descumprimento dos prazos e condições determinados neste Termo de Referência, a(s) empresa(s) contratada(s) estará(ão) sujeita(s) às penalidades previstas na legislação vigente, bem como nos instrumentos convocatório e contratual, conforme o caso.

Assinaturas da Equipe de Planejamento da Contratação

Mozart Fernandes Moreira Lima **Integrante Técnico**	**Gustavo Oliveira Heitmann** **Integrante Administrativo**
Luiz Gustavo Marques Florindo **Integrante Demandante**	
Data: 25/09/2020	

[g1]Definição do objeto e de sua natureza, de forma sucinta, precisa e clara. Fazer menção à vigência contratual (serviço) e utilização do SRP (se for o caso). OBS: A descrição do objeto será utilizada na publicação do aviso de edital.

[g2]Indicação da motivação (necessidade) da contratação, dos resultados (objetivos) a serem alcançados por meio da contratação e dos benefícios diretos e indiretos resultantes da adoção da STIC, que deverá estar em conformidade com as informações apresentadas no Documento de Oficialização da Demanda (DOD) e na Análise de Viabilidade da Contratação.

[g3]Indicação do alinhamento entre a contratação e o Planejamento Estratégico Institucional do TRE (PEI) ou Planos de Tecnologia da Informação e Comunicação do TRE (PETIC ou PDTIC), baseado nas informações presentes no Documento de Oficialização da Demanda (DOD) e nos Estudos Preliminares.

[g4]Indicação do documento ou processo administrativo que contém os referidos estudos. Se possível, juntá-los aos autos.

[g5]Demonstração da relação entre a demanda prevista e a quantidade de bens ou serviços a serem contratados, com base nos Estudos Preliminares. Quantificação ou estimativa prévia do volume de serviços demandados ou quantidade de bens a serem fornecidos, para comparação e controle. Na contratação de serviços, caso não seja utilizada a unidade de serviço técnico-UST, deverá ser apresentada a justificativa técnica para a adoção de outro tipo de métrica. SÚMULA TCU Nº 269: Nas contratações para a prestação de serviços de tecnologia da informação, a remuneração deve estar vinculada a resultados ou ao atendimento de níveis de serviço, admitindo-se o pagamento por hora trabalhada ou por posto de serviço somente quando as características do objeto não o permitirem, hipótese em que a excepcionalidade deve estar prévia e adequadamente justificada nos respectivos processos administrativos.

[g6]Indicação das razões que motivaram a escolha da STIC a ser contratada, explicitando os requisitos do negócio e tecnológicos que serão atendidos pelos bens ou serviços a serem entregues, bem como da vantajosidade técnica e econômica da escolha.

[g7]Deverá ser justificada a utilização do Sistema de Registro de Preços considerando as hipóteses legais previstas nos incisos I a IV do artigo 3º, do Decreto 7.892/2013). Exemplo: vide PAD 1700126/2017- Aquisição de material de expediente (SRP)

[g8]Deverá ser indicado o parcelamento ou não dos itens que compõem a STIC, evidenciando a viabilidade técnica e econômica, tendo como parâmetro a ampliação da competitividade, sem perda da economia de escala. Também deverá ser justificada a forma escolhida para adjudicação do objeto, se por item, se por lote, se por preço global, por exemplo, demonstrando se a STIC pode ser adjudicada a uma ou a várias empresas.

[g9]Deverá ser indicada a aplicação de direito de Preferência, sempre que cabível, nos termos da legislação vigente.

(Decreto 7174 ou outro normativo. Obs: Decretos de margem de preferência objeto do Decreto 8626/2016 tiveram vigência final fixada em 31.12.2016

[g10]Indicação da especificação técnica detalhada do objeto, necessária para gerar os resultados pretendidos com a contratação, bem como a indicação das normas técnicas e legais, caso existam, às quais a STIC deverá estar aderente.

[s11]Indicar os requisitos de negócio, técnicos e demais requisitos definidos nos estudos preliminares.

[g12]Descrição das rotinas de execução, envolvendo a dinâmica de entrega ou fornecimento da STIC contratada, com a indicação das etapas, da logística de implantação, prazos, horários e locais de entrega/prestação dos serviços, quando aplicáveis; documentação exigida, observando modelos adotados pela contratante; papeis e responsabilidades específicos para a aquela contratação, a serem desempenhados pela contratante e pela contratada; bem como os mecanismos formais de comunicação entre a contratante e a contratada para troca de informações, inclusive para a solicitação do fornecimento dos bens ou prestação dos serviços, adotando-se, preferencialmente, as Ordens de Serviço ou de Fornecimento de Bens. Caso necessário, poderão ser confeccionados e anexados ao Termo de Referência ou Projeto Básico os modelos de documentos a serem utilizados para solicitação de bens ou serviços.

[g13]Elaboração do Termo de Compromisso de Manutenção de Sigilo, a ser assinado pelo representante legal da contratada e do Termo de Ciência e Aceite das Condições de Manutenção de Sigilo, a ser assinado por todos os empregados diretamente envolvidos na contratação, sempre que a contratada fizer uso de quaisquer ativos da contratante, no fornecimento da solução.

[g14]Inserir, quando for o caso, requisitos de qualificação técnicas a serem comprovados. OBS: A comprovação de certificação profissional em TI somente pode ser exigida como obrigação contratual, em prazo a ser asssinaldado a contar da data de início de vigência do contrato.

[g15]Deverá ser indicada a vigência do contrato, incluindo o período de garantia dos bens ou da prestação dos serviços contratados (prazo de garantia superior a 90 dias deverá ser justificado nos autos). Sempre que a vigência contratual ultrapassar 12 meses (somente nos casos de serviços contínuos

ou locação de equipamentos), deverá ser apresentada justificativa e demonstrada a vantajosidade técnica e econômica

[g16]**Definição das obrigações da CONTRATANTE, sempre que necessário, a obrigação de:**

a) Nomear Gestor e Fiscais Técnico, Administrativo e Demandante do contrato para acompanhar e fiscalizar a execução dos contratos;

b) Encaminhar formalmente a demanda, preferencialmente por meio de Ordem de Serviço ou Fornecimento de Bens, de acordo com os critérios estabelecidos no Termo de Referência ou Projeto Básico;

c) Receber o objeto fornecido pela CONTRATADA que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;

d) Aplicar à CONTRATADA as sanções administrativas regulamentares e contratuais cabíveis, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando se tratar de contrato oriundo de Ata de Registro de Preços;

e) Liquidar a despesa e efetuar o pagamento à CONTRATADA, dentro dos prazos preestabelecidos em Contrato;

f) Comunicar à CONTRATADA todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC.

[g17] Definição das obrigações da CONTRATADA, quando cabível, a obrigação de:

a) Indicar, formalmente, preposto apto a representá-la junto à CONTRATANTE, que deverá responder pela fiel execução do contrato;

b) Atender prontamente quaisquer orientações e exigências do gestor do contrato, inerentes à execução do objeto contratual;

c) Reparar quaisquer danos diretamente causados à CONTRATANTE ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual;

d) Propiciar todos os meios e facilidades necessárias à fiscalização da solução de TIC pela CONTRATANTE;

e) Manter, durante toda a execução do contrato, as mesmas condições da habilitação;

f) Manter, quando especificada e durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TIC;

g) Manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato;

h) Fornecer, sempre que solicitado, amostra para realização de Prova de Conceito (POC) para fins de comprovação de atendimento das especificações técnicas;

i) Ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos entregues ao longo do contrato, incluindo a documentação, os modelos de dados e as bases de dados, à Administração; e

j) Proceder à transferência de conhecimento à CONTRATANTE, ao término da relação contratual, com vistas à minimização da dependência técnica entre eles.

[g18]Indicação de como se dará o pagamento dos bens ou serviços recebidos definitivamente.

[g19]Abranger quando for o caso, métricas, indicadores e níveis mínimos de serviços aceitáveis para os principais elementos que compõem a STIC. (IN 04 /2014, art. 20, I)

[g20]A indicação para fins de elaboração dos Termos de Recebimento Provisório e Definitivo**,** conforme disposto no art. 73, ressalvadas as hipóteses do art. 74, ambos da Lei 8.666/1993, abrangendo a forma de avaliação da qualidade e adequação da Solução de Tecnologia da Informação às especificações funcionais e tecnológicas estabelecidas, observando, se preciso, a confecção de Listas de Verificação e de roteiros de testes, para subsidiar a ação dos fiscais do contrato. (IN 04 /2014, art. 20, II, a, 4)

[g21]Fixação, quando for o caso, dos valores e procedimentos para retenção ou glosa no pagamento, sem prejuízo das sanções cabíveis, que só deverá ocorrer quando a contratada:

a. Não atingir os valores mínimos aceitáveis fixados nos Critérios de Aceitação, não produzir os resultados ou deixar de executar as atividades contratadas; ou
b. Deixar de utilizar materiais e recursos humanos exigidos para fornecimento da Solução de Tecnologia da Informação, ou utilizá-los com qualidade ou quantidade inferior à demandada.

[g22]Definição detalhada das sanções administrativas, de acordo com os arts. 86, 87 e 88 da Lei 8.666, de 1993 c/c o art. 7º da Lei nº 10.520, de 2002, observando, sempre que cabível:

a. Vinculação aos termos contratuais;
b. Proporcionalidade das sanções previstas ao grau do prejuízo causado pelo descumprimento das respectivas obrigações;
c. As situações em que advertências ou multas serão aplicadas, com seus percentuais correspondentes, que obedecerão a uma escala gradual para as sanções recorrentes;
d. As situações em que o contrato será rescindido por parte da Administração, devido ao não atendimento de termos contratuais, da recorrência de aplicação de multas ou outros motivos;
e. As situações em que a contratada será declarada inidônea para licitar ou contratar com a Administração, conforme previsto em lei.

Em 23 de outubro de 2020

Documento assinado eletronicamente por **GUSTAVO OLIVEIRA HEITMANN**, **Técnico Judiciário**, em 23/10/2020, às 17:04, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **MOZART FERNANDES MOREIRA LIMA**, **Técnico Judiciário**, em 23/10/2020, às 17:13, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **LUIZ GUSTAVO MARQUES FLORINDO**, **Analista Judiciário**, em 23/10/2020, às 17:29, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade deste documento pode ser conferida no site https://sei.tre-mg.jus.br/controlador_externo.php?acao=documento_conferir&acao_origem=documento_conferir&lang=pt_BR&id_orgao_acesso_externo=0, informando o código verificador **1079102** e o código CRC **B63C4BDA**.

TRIBUNAL REGIONAL ELEITORAL DO ESPÍRITO SANTO
Rua João Batista Parra, 575 - Bairro Praia do Suá - CEP 29052-123 - Vitória - ES

ESTUDO TÉCNICO PRELIMINAR (DEMANDAS DE TIC) Nº 15/2020 - TRE-ES/PRE/DG/STI/CIS/SRCD

(este documento deve seguir as orientações da Resolução TRE/ES nº 261/2018)

SUMÁRIO

ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO

1 - CARACTERIZAÇÃO DA DEMANDA

1.1 - Descrição Sucinta

Aquisição de uma solução unificada para gestão de vulnerabilidades dos ativos de tecnologia da informação e aplicações web do TRE-ES.

1.2 - Justificativa da necessidade e Resultados

A gestão de vulnerabilidades é um processo que se preocupa com a descoberta e remediação de vulnerabilidades que podem estar presentes nos sistemas de informação. Uma vulnerabilidade pode surgir pela utilização de uma versão comprometida de um software ou por uma configuração inadequada de uma aplicação. Essa vulnerabilidade pode ser explorada por um atacante para prejudicar a disponibilidade, integridade e confidencialidade dos ativos de informação. Existem inúmeras ações maliciosas que podem explorar um vasto número vulnerabilidades existentes. Dentre elas podemos citar:

- Utilização de usuários e senhas padrões: A maioria de aplicações possuem usuários e senhas padrões, de conhecimento público, que caso não sejam alteradas ou desabilitadas podem ser utilizadas por invasores para acessar os sistemas e obter informações importantes ou sigilosas;

- Problemas de criptografia: Ocorre quando aplicações ou sites utilizam algorítmos de criptografia "fracos" que possibilitem ao invasor quebrar a chave e obter dados sensíveis que podem ser utilizados para obter acesso a servidores, banco de dados, sistemas essenciais, etc.

- CRLF Injection: Ocorre quando um invasor pode injetar uma sequência CRLF - "Carriage Return (Retorno de carro)" e "Line Field (Avanço de linha)" - em um fluxo HTTP. Ao introduzir esta injeção de CRLF inesperada, o invasor é capaz de explorar vulnerabilidades de CRLF de forma mal-intencionada para manipular as funções do aplicativo da web.

- Cross-site Scripting (XSS): Acontece quando um invasor explora uma área de um site que possui conteúdos dinâmicos. O invasor consegue rodar seu código dentro do site da vítima, causando o roubo de contas de usuários, controle do navegador da vítima, e muito mais. Esse problema é comum em formulários de contato que permitem a inserção de caracteres utilizados em linguagens de programação como pontos de interrogação ou barras.

- Acesso a diretórios restritos: Ocorre quando o invasor consegue se aproveitar de sites desprotegidos, conseguindo acesso a um grande número de arquivos de sistema, tendo acesso a nome de usuários, senhas, documentos importantes e até mesmo o código fonte do site/aplicativo.

- SQL Injection: Ocorre quando o invasor se aproveita de falhas em sistemas que interagem com bases de dados através de comandos SQL, onde o atacante consegue inserir uma instrução SQL personalizada e indevida dentro de uma consulta (SQL query) através da entradas de dados de uma aplicação, como formulários ou páginas de uma aplicação.

- Varredura em redes (*Scan*): Varredura em redes, ou *scan*, é uma técnica que consiste em efetuar buscas minuciosas em redes, com o objetivo de identificar computadores ativos e coletar informações sobre eles como, por exemplo, serviços disponibilizados e programas instalados. Com base nas informações coletadas é possível associar possíveis vulnerabilidades aos serviços disponibilizados e aos programas instalados nos computadores ativos detectados.

- Interceptação de tráfego (*Sniffing*): Interceptação de tráfego, ou *sniffing*, é uma técnica que consiste em inspecionar os dados trafegados em redes de computadores, por meio do uso de programas específicos chamados de *sniffers*.

- Força bruta (*Brute force*): Um ataque de força bruta, ou *brute force*, consiste em adivinhar, por tentativa e erro, um nome de usuário e senha e, assim, executar processos e acessar *sites*, computadores e serviços em nome e com os mesmos privilégios deste usuário.

- Negação de serviço (DoS e DDoS): Negação de serviço, ou DoS (*Denial of Service*), é uma técnica pela qual um atacante utiliza um computador para tirar de operação um serviço, um computador ou uma rede conectada à Internet. Quando utilizada de forma coordenada e distribuída, ou seja, quando um conjunto de computadores é utilizado no ataque, recebe o nome de negação de serviço distribuído, ou DDoS (*Distributed Denial of Service*). O objetivo destes ataques não é invadir e nem coletar informações, mas sim exaurir recursos e causar indisponibilidades ao alvo.

Devido à complexidade e quantidade de ativos de informação utilizados no nosso ambiente de TIC, o processo de gestão de vulnerabilidades necessita ser suportado por uma solução de gestão de vulnerabilidades.

Um grupo da Justiça Eleitoral, formado pelo TSE e 8 (oito) Tribunais Regionais, vem, nos últimos 2 meses, estudando soluções que possam suprir essa demanda, que é essencial para a Segurança da Informação no âmbito da Justiça Eleitoral. O TRE/PB foi selecionado para conduzir o processo de aquisição (órgão gerenciador) pelo sistema de registro de preços, cabendo ao TSE e outros TREs ingressar no processo de aquisição (órgãos participantes) por ocasião do registro da IRP (Intenção de Registro de Preços) no sistema Comprasnet. Cabe ressaltar que este Estudo Técnico está em total consonância com o documento de planejamento que integra o processo do TRE/PB (SEI TRE/PB 0008787-53.2020.6.15.8000) e sua produção neste processo tem como objetivo:

1. Mostrar o alinhamento da aquisição com o Planejamento Estratégico do Tribunal;

2. Justificar a necessidade de aquisição da solução e apresentar os resultados esperados;

3. Alinhar a demanda do TRE/ES com a STIC objeto da aquisição, apontando os itens específicos necessários a este TRE, dentre os disponíveis no Termo de Referência produzido no âmbito do processo SEI TRE/PB 0008787-53.2020.6.15.8000)

Quanto aos requisitos funcionais e tecnológicos da solução, não há qualquer diferença entre este estudo e o ETP produzido pelo orgão gerenciador da ARP, o TRE/PB.

Os objetivos (resultados) esperados são:

- Identificação e priorização de tratamento de vulnerabilidades nos ativos de TIC (roteadores, switches, estações de trabalho, hosts de virtualização, bancos de dados, maquinas virtuais, sistemas operacionais, servidores de aplicação, aplicações web, etc) do TRE-ES;

- Redução do nível de risco através da redução da probabilidade de ameaças explorarem vulnerabilidades de nossos ativos.

2 - ESPECIFICAÇÃO DOS REQUISITOS FUNCIONAIS

2.1 - Requisitos Relacionados ao Negócio

- Gerenciamento de Vulnerabilidades em Sistemas Operacionais: 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*;*

- Gerenciamento de Vulnerabilidades em Sistemas e páginas Web: 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;

- Emissões de Relatórios: emitir relatórios de acompanhamento dos testes e das vulnerabilidades encontradas, apontando quando forem solucionadas;

2.2 - Requisitos de Capacitação, Ambientais, Culturais e Sociais

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

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;

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;

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.

2.3 - Requisitos de Manutenção

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

2.4 - Requisitos Temporais

As licenças adquiridas devem ser vitalícias (perpétuas) não havendo necessidade de renovação ao longo do tempo;

A garantia de atualização do software deve ser de, no mínimo, 36 (trinta e seis) meses;

2.5 - Requisitos de Segurança

A empresa contratada deverá respeitar as diretrizes constantes da Política de Segurança da Informação 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 Espírito Santo aos quais tiver acesso em decorrência do objeto da presente contratação, ficando terminantemente proibida de fazer uso ou revelação destes sob qualquer justificativa;

O Tribunal Regional Eleitoral da Espírito Santo terá propriedade sobre todos os documentos e procedimentos operacionais produzidos no escopo da presente contratação;

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

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.

3. ESPECIFICAÇÃO DOS REQUISITOS TECNOLÓGICOS

3.1 - Características Gerais

3.1.1 - A solução deve estar licenciada e nela devem estar 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;

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

3.1.3 - A solução de gestão de vulnerabilidades deve suportar varreduras de dispositivos de IoT;

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

3.1.5 - 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;

3.1.6 - Deve atribuir a todas as vulnerabilidades uma severidade baseada no CVSSv3 score;

3.1.7 - 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;

3.1.8 - A solução deve fornecer criptografia de ponta a ponta dos dados de vulnerabilidades;

3.1.9 - A solução deve possuir a capacidade de armazenar informações dos ativos descobertos no ambiente;

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

- Por sistema operacional;
- Por um determinado software instalado;
- Por Ativos impactados por uma determinada vulnerabilidade.

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

3.1.12 - Deve permitir aceitar o risco de uma determinada vulnerabilidade encontrada no ambiente;

3.1.13 - Possibilitar alterar a criticidade de determinada vulnerabilidade de forma manual;

3.1.14 - A solução deve possuir um sistema de pontuação e priorização das vulnerabilidades;

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

3.1.6 - O sistema de pontuação e priorização de vulnerabilidades deve avaliar no mínimo as seguintes características:

- CVSSv3 Impact Score;
- Idade da Vulnerabilidade;
- Se existe ameaça ou exploit que explore a vulnerabilidade;
- Número de produtos afetados pela vulnerabilidade;

3.1.17 -Deve ser capaz de fazer a correlação em tempo real de ameaças ativas contra vulnerabilidades encontradas, incluindo feeds de inteligência de ameaças ao vivo;

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

3.1.19 - 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;

3.1.20 - A solução deve permitir a instalação de agentes em estações de trabalho e servidores, para varredura diretamente no sistema operacional;

3.1.21 - A solução deve possuir conectores para, no mínimo, as seguintes plataformas:

- Amazon Web Service (AWS);
- Microsoft Azure;
- Google Clound Platform.

3.1.22 - A solução deve ser capaz de produzir relatórios nos seguintes formatos: PDF, CSV, HTML e no formato de texto que poderá ser DOCX ou RTF;

3.1.23 - A solução deve possuir recurso de monitoria passiva do tráfego de rede para identificação de anomalias, novos dispositivos e desvios de padrões observados;

3.1.24 - A solução deve ser licenciada para o uso ilimitado de sensores passivos de rede para realizar o monitoramento em tempo real;

3.1.25 - A solução deve possuir sensores, no mínimo, com as seguintes funcionalidades:

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

3.1.26 - Deve ser possível determinar em tempo real quais portas de serviços (UDP/TCP) estão abertas em determinado ativo;

3.1.27 - A solução deve ser capaz de realizar em tempo real a descoberta de novos ativos para no minímo:

- Bancos de dados;
- Hypervisors (no mímino VMWare ESX/ESXi);
- Dispositivos móveis;
- Dispositivos de rede;
- Endpoints;
- Aplicações;

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

3.1.29 - Permitir identificar vulnerabilidades associadas a servidores SQL no tráfego de rede;

3.1.30 - A solução deve possuir interface para integração com as principais soluções de SIEM de mercado, tais como IBM QRadar, Microfocus ArcSight e Splunk.

3.1.31 - 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.

3.1.32 - A atualização das ameaças deve ocorrer diariamente e sem interrupção dos serviços.

3.1.33 - Configuração de segurança e acesso à gerência da solução:

- Todos os dados armazenados nos servidores da solução devem ser criptografados e possuir logs de acesso;
- Os dados em transito devem usar ao menos o algoritimo TLS 1.2 de chave 2048 bits;
- Os dados em transito devem ser criptografados ao menos com o algoritimo AES-128 bits;
- Os algoritimos de hash devem usar ao menos o algoritimo SHA-256;
- Será aceito como comprovação critérios de criptografia publicação em site do fabricante ou declaração do próprio fabricante;
- Os dados armazenados devem ser criptografados ao menos com o algoritimo AES-256 bits;
- Somente servidores da Contratante ou pessoa por ela autorizada poderão ter acesso aos dados da solução;

- A solução deve permitir a criação de, no mínimo, 20 contas para gerência e acesso aos relatórios, sem custo adicional;
- 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).

3.1.34 - Todas as licenças de uso de software devem ser registradas, na data da entrega, em nome da Contratante no site do fabricante.

3.1.35 - Dos Relatórios:

- Deve ser capaz de executar relatórios periódicos de acordo com a frequência estabelecida pelo administrador, bem como a geração de relatórios sob demanda;
- A solução deve possibilitar a criação de relatórios baseados na seleção de ativos, permitindo inclusive a seleção de todos os ativos existentes;
- Deve suportar a criação de relatórios criptografados (protegidos por senha configurável) ;
- A solução deve suportar o envio automático de relatórios para destinatários específicos;
- Deve ser possível definir a frequência na geração dos relatórios para no mínimo: Diário, Mensal, Semanal e Anual;
- Permitir especificar níveis de permissão nos relatórios para usuários e grupos específicos;
- A solução deve fornecer relatórios do tipo “scorecard” para as partes interessadas da empresa;
- A solução deve fornecer relatórios de correções aplicadas, classificados pelos seguintes critérios: grupo de ativos, usuários e vulnerabilidades;

3.1.36 - A solução deve permitir mecanismo de varredura baseado em inferência com técnicas de varredura não intrusivas;

3.1.37 - A solução deve possuir ou permitir a criação de relatórios com as seguintes informações:

- Hosts verificados sem credenciais;
- Top 100 Vulnerabilidades mais criticas;
- Top 10 Hosts infectados por Malwares;
- Hosts exploráveis por Malwares;
- Total de vulnerabilidades que podem ser exploradas pelo Metasploit;
- Vulnerabilidades críticas e exploráveis;
- Máquinas com vulnerabilidades que podem ser exploradas;

3.1.38 - A solução deve possuir dashboards customizáveis onde o administrador pode criar, editar ou remover painéis de acordo com a necessidade;

3.1.39 - A solução deve ser capaz de inventariar todos os ativos da rede local e publicados na Internet, sem limites de endereços IPs.

3.1.40 - A plataforma de software deve ser capaz de realizar varreduras (scans) de vulnerabilidades para no mínimo 250 IPs;

3.1.41 - A plataforma de software deve ser licenciada para um número ilimitado de scanners (prevendo redundância);

3.1.42 - Deve permitir a configuração de vários painéis e widgets;

3.1.43 - Deve ser capaz de medir e reportar ameaças;

3.1.44 - Deve ser capaz de visualizar ameaças críticas ao ambiente monitorado;

3.1.45 - 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;

3.1.46 - A plataforma de software deve suportar vários mecanismos de varredura distribuídos em

diferentes localidades e regiões e gerenciar todos por uma console central;

3.1.47 - 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;

3.1.48 - A plataforma de software deve permitir o monitoramento através de agentes instalados, até o limite de licenças adquiridas, para varredura diretamente no sistema operacional.

3.1.49 - 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.

3.1.50 - 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;

3.1.51 - 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;

3.1.52 - A plataforma de software deve ser configurável para permitir a otimização das parametrizações de varredura;

3.1.53 - 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;

3.1.54 - A plataforma de software deve fornecer a capacidade de escalar privilégios nos destinos, do acesso de usuário padrão até acesso de sistema ou administrativo;

3.1.55 - A plataforma de software deve ser capaz de realizar pesquisas de dados confidenciais.

3.1.56 - A solução deve possuir módulo para realizar varreduras de vulnerabilidade Web:

3.1.56.1 - A solução de análise deve realizar varreduras de vulnerabilidades para no mínimo 10 aplicações Web, cobrindo no mínimo, mas não limitando-se a base de ameaças apontadas pelo OWASP Top 10, CWE e WASC;
3.1.56.2 - A solução de análise deve ser capaz de analisar, testar e reportar falhas de segurança em aplicações Web;
3.1.56.3 - A solução de análise deverá ser capaz de executar varreduras em sistemas Web através de seus endereços IP ou FQDN (DNS);
3.1.56.4 - A solução de análise deve ser capaz de identificar vulnerabilidades de divulgação de dados, como vazamento de informações de identificação pessoal;
3.1.56.5 - 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;

3.1.56.6 - Deverá também permitir a execução da função crawler, que consiste na navegação para descoberta das URLs existentes na aplicação;
3.1.56.7 - A solução de análise deve suportar a integração com o softwares de automação de testes para permitir sequências de autenticação complexas;
3.1.56.8 - A solução de análise deve ser capaz de realizar testes/varreduras em aplicações separadas, simultaneamente limitadas ao número de licenças;
3.1.56.9 - Suporte a ferramentas para construção de requisições e análise de respostas de aplicações WEB, API's e WebServices, tais como Postman Collections;
3.1.56.10 - A solução de análise deve oferecer suporte à capacidade de testar novamente a

vulnerabilidade específica que foi detectada anteriormente no aplicativo Web;
3.1.56.11 - Deve ser capaz de utilizar scripts customizados de crawling com parâmetros definidos pelo usuário;
3.1.56.12 - Deve ser capaz de excluir determinadas URLs da varredura através de expressões regulares;
3.1.56.13- Deve ser capaz de excluir determinados tipos de arquivos através de suas extensões;
3.1.56.14 - 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;

3.1.56.15 - Deve ser capaz de agendar a varredura e determinar sua frequência entre uma única vez, diária, semanal, mensal e anual;
3.1.56.16 - Deve suportar o envio de notificações por email;
3.1.56.17 - Deverá ser compatível com avaliação de web services REST e SOAP;
3.1.56.18 - A solução de análise deve suportar os seguintes esquemas de autenticação:

a) Autenticação Básica (Digest);
b) NTLM;
c) Autenticação de Cookies;

3.1.56.19 - Deve ser capaz de importar scripts de autenticação previamente configurados pelo usuário;
3.1.56.20 - 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;
3.1.56.21 - Os resultados devem ser apresentados agregados por vulnerabilidades ou por aplicações;
3.1.56.22 - Para cada vulnerabilidade encontrada, deve ser exibido detalhes e evidências;
3.1.56.23 - Cada vulnerabilidade encontrada deve conter também soluções propostas para mitigação ou remediação;
3.1.56.24 - 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.

3.1.56.25 - 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;
x) Redmine.

4. IDENTIFICAÇÃO E COMPARAÇÃO DAS SOLUÇÕES ADERENTES AOS REQUISITOS

As soluções presentes neste estudo resumem-se às seguintes opções.

4.1 - Utilização de softwares livres

Descrição da Solução: Utilização de ferramentas livres ou gratuitas, como os softwares OpenVas e Nmap.

Fornecedor da Solução: Comunidades Open Source e páginas específicas dos projetos.

Órgão /Entidade Proprietário da Solução: Não se aplica à presente contratação.

Orçamento da Solução: Gratuita.

Aderência da Solução ao MNI: Não se aplica à presente contratação.

Aderência da Solução ao ICP-Brasil: Não se aplica à presente contratação.

Aderência da Solução ao Moreq-Jus: Não se aplica à presente contratação.

4.2 - Solução paga com gerenciamento e armazenamento na nuvem (On Cloud)

Descrição da Solução: Aquisição de software de gerenciamento de vulnerabilidades e análise dinâmica de aplicações web baseado em nuvem, com modelo de subscrição por 36 meses.

Fornecedores da Solução: Empresas de mercado.

Órgão /Entidade Proprietário da Solução: Não se aplica à presente contratação.

Orçamento da Solução: Estimamos o valor da contratação em R$ 234.930,00 (Duzentos e trinta e quatro mil novecentos e trinta reais)

Aderência da Solução ao MNI: Não se aplica à presente contratação.

Aderência da Solução ao ICP-Brasil: Não se aplica à presente contratação.

Aderência da Solução ao Moreq-Jus: Não se aplica à presente contratação.

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

Descrição da solução: 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 36 meses ou de licença perpetua com suporte de 36 meses.

Fornecedores da Solução: Empresas de mercado.

Órgão /Entidade Proprietário da Solução: Não se aplica à presente contratação.

Orçamento da Solução: Estimamos o valor da contratação em R$ 165.404,96 (Cento e sessenta e cinco mil quatrocentos e quatro reais e noventa e seis centavos)

Aderência da Solução ao MNI: Não se aplica à presente contratação.

Aderência da Solução ao ICP-Brasil: Não se aplica à presente contratação.

Aderência da Solução ao Moreq-Jus: Não se aplica à presente contratação.

5 - INDICAÇÃO DA STIC 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 como os 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 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 premise) 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. Esta solução consegue fazer o gerenciamento de vulnerabilidades em ativos de tecnologia da informação além de testes em aplicações Web. Outro ponto favorável à solução 3 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, por ser o menor preço e pelo 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.

5.1 - Descrição da Solução

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 36 meses ou de licença perpetua com suporte de 36 meses.

Valor Estimado (baseado na melhor proposta on premise): R$ 165.404,96 (Cento e sessenta e cinco mil quatrocentos e quatro reais e noventa e seis centavos).

5.2 - Justificativa/Motivação da Escolha

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.

5.3 - Aderência aos Requisitos

Os requisitos tecnológicos estão aderentes aos requisitos funcionais estabelecidos pelo demandante.

5.4 - Relação entre a Demanda Prevista e a STIC

O TRE-ES possui aproximadamente 210 (duzentos e dez) ativos de rede (servidores, switches, firewalls, appliances, storages, bibliotecas de fitas, controladoras wifi, Access Points, etc.) que estão suscetíveis a vulnerabilidades e que precisam ser analisados constantemente para a remoção das mesmas. Considerando que nas propostas são oferecidas faixas de licenciamento para 128, 250, 250, 500 e 1000 endereços IP's, a faixa de licenciamento de 250 IPs foi escolhida por ser a que atende a demanda.

Hoje possuímos aplicações web em produção disponibilizadas na internet em 9 *FQDN's* (Full Qualified Domain Name) distintos. Considerando que nas propostas são oferecidas faixas de licenciamento para análise dinâmica de aplicações web em 5, 10 e 40 domínios FQDN's, a faixa de licenciamento de 10 domínios foi escolhida por ser a que atende a demanda.

Assim, para atender a demanda existente precisamos realizar a contratação dos seguintes itens:

ITEM	QUANTIDADE
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
Licenciamento para solução de análise dinâmica em aplicações Web, pacote para no mínimo 10 domínios (FQDN), por 36 meses de uso e suporte do fabricante.	1
Instalação e configuração	1
Repasse Tecnológico com período mínimo de 20 horas	1

6 - INDICAÇÃO DA NECESSIDADE DE ADEQUAÇÃO AMBIENTAL

Não existem necessidades de adequação ambiental.

ANÁLISE DE RISCOS

7 - IDENTIFICAÇÃO DOS RISCOS

O principal risco identificado foi:

- Não cumprimento do prazo de entrega pela contratada.

8 - RELAÇÃO DOS RISCOS E AÇÕES DE MITIGAÇÃO

RISCO 1	NÃO CUMPRIMENTO DO PRAZO DE ENTREGA PELA CONTRATADA	
Probabilidade (Alta, média ou baixa)	Baixa	
	Efeito (Dano)	***Impacto**
1	Atraso na ativação dos serviços	Baixo
	Ações de Mitigação e Contingência	**Responsável**
1	Acompanhar rigorosamente junto à empresa o andamento da operação de entrega	Integrante técnico

*Impacto (Baixo, Médio ou Alto)

ANÁLISE DE SUSTENTAÇÃO DO CONTRATO

9. RECURSOS MATERIAIS E HUMANOS

Trata-se de aquisição de licenciamento de software. A instalação e configuração inicial serão realizadas pela contratada. A contratada também será responsável pelo repasse de conhecimento para operação da solução com período mínimo de 20 horas.

10. DESCONTINUIDADE DO FORNECIMENTO

Não se aplica. Compra de licenciamento de software em parcela única.

EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO

Integrante Demandante: Rommel Baia Silva (substituto: Lucas Ribeiro Carlin)

Integrante Técnico: Lucas Ribeiro Carlin (substituto: Rommel Baia Silva)

Integrante Administrativo: Marcos Venturott Ferreira (substituto: Carlos Alberto da Rocha Padua Filho)

Vitória, 02 de setembro de 2020.

Documento assinado eletronicamente por **CARLOS ALBERTO DA ROCHA PADUA FILHO**, **Coordenador(a)**, em 16/09/2020, às 14:39, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **LUCAS RIBEIRO CARLIN**, **Técnico Judiciário**, em 16/09/2020, às 14:56, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **ROMMEL BAIA SILVA**, **Chefe de Seção**, em 16/09/2020, às 14:59, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://sei.tre-es.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0412192** e o código CRC **1C8509DC**.

TRIBUNAL REGIONAL ELEITORAL DE MATO GROSSO DO SUL
R. Desembargador Leão Neto do Carmo, 23 - Bairro Parque dos Poderes - CEP 79037-100 - Campo Grande - MS

ESTUDO PRELIMINAR

1 ESTUDOS PRELIMINARES

1.1 SOLUÇÃO DE TI A CONTRATAR

O presente estudo preliminar visa a implantação de uma Ferramenta de Gestão de Vulnerabilidades.

1.2 EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO

A equipe responsável pelo planejamento da contratação é composta pelos seguintes membros:

Nome	Lotação	Tipo	Email
Gustavo Pinho	SSOP/COINF/STI	Técnico	gustavo.pinho@tre-ms.jus.br
Maria Júlia de Arruda Mestieri	SAF/CRM/SLC	Administrativo	julia.mestieri@tre-ms.jus.br

1.3 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.

2 ANÁLISE DA VIABILIDADE DA CONTRATAÇÃO (ART.14)

2.1 DEFINIÇÃO E ESPECIFICAÇÃO DOS REQUISITOS DA DEMANDA (ART. 14, I)

Item 1 - Solução de Segurança para Datacenter		
Subitem	**Descrição**	**Qtde (Unidade)**
1.1	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 pelo fabricante.	05 (licença)
1.2	Licenciamento para solução de análise dinâmica em aplicações Web, pacote para no mínimo 5 domínios (FQDN), por 36 meses de uso e suporte pelo fabricante.	02 (licença)
1.3	Instalação e configuração da solução.	01 (unidade)
1.4	Repasse tecnológico, com período mínimo de 20 horas.	01 (unidade)
1.5	4 Horas de Serviço Especializado.	50 (unidade)

Requisitos Tecnológicos
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;
2. A solução deve possuir recurso de varredura ativa, onde o scanner comunica-se com os alvos (ativos) através da rede;
3. A solução de gestão de vulnerabilidades deve suportar varreduras de dispositivos de IoT;
4. Deve ser capaz de identificar no mínimo 50.000 CVEs (Common Vulnerabilities and Exposures);
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;
6. Deve atribuir a todas as vulnerabilidades uma severidade baseada no CVSSv3 score;
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;
8. A solução deve fornecer criptografia de ponta a ponta dos dados de vulnerabilidades;
9. A solução deve possuir a capacidade de armazenar informações dos ativos descobertos no ambiente;
10. Deve possuir um sistema de busca de informações de um determinado ativo com no mínimos as seguintes características:
    10.1. Por sistema operacional;
    10.2. Por um determinado software instalado;

10.3. Por Ativos impactados por uma determinada vulnerabilidade.
11. A solução deve possuir suporte para a adição de detecções personalizadas usando o OVAL (Open Vulnerability Assessment Language);
12. Deve permitir aceitar o risco de uma determinada vulnerabilidade encontrada no ambiente;
13. Possibilitar alterar a criticidade de determinada vulnerabilidade de forma manual;
14. A solução deve possuir um sistema de pontuação e priorização das vulnerabilidades;
15. A solução deve ser capaz de aplicar algoritmos de aprendizagem de máquina (machine learning) para analisar as características relacionadas a vulnerabilidades;
16. O sistema de pontuação e priorização de vulnerabilidades deve avaliar no mínimo as seguintes características:
16.1. CVSSv3 Impact Score;
16.2. Idade da Vulnerabilidade;
16.3. Se existe ameaça ou exploit que explore a vulnerabilidade;
16.4. Número de produtos afetados pela vulnerabilidade;
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;
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;
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;
20. A solução deve permitir a instalação de agentes em estações de trabalho e servidores, para varredura diretamente no sistema operacional;
21. A solução deve possuir conectores para, no mínimo, as seguintes plataformas:
a) Amazon Web Service (AWS);
b) Microsoft Azure;
c) Google Clound Platform.
22. A solução deve ser capaz de produzir relatórios nos seguintes formatos: PDF, CSV, HTML e no formato de texto que poderá ser DOCX ou RTF;
23. A solução deve possuir recurso de monitoria passiva do tráfego de rede para identificação de anomalias, novos dispositivos e desvios de padrões observados;
24. A solução deve ser licenciada para o uso ilimitado de sensores passivos de rede para realizar o monitoramento em tempo real;
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;
26. Deve ser possível determinar em tempo real quais portas de serviços (UDP/TCP) estão abertas em determinado ativo;
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;
28. A solução deve ser capaz de em tempo real detectar logins e downloads de arquivos em um compartilhamento de rede;

29. Permitir identificar vulnerabilidades associadas a servidores SQL no tráfego de rede;
30. A solução deve possuir interface para integração com as principais soluções de SIEM de mercado, tais como IBM QRadar, Microfocus ArcSight e Splunk.
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.
32. A atualização das ameaças deve ocorrer diariamente e sem interrupção dos serviços.
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;
f) Os dados armazenados devem ser criptografados ao menos com o algoritimo AES-256 bits;
g) Somente servidores da Contratante ou pessoa por ela autorizada poderão ter acesso aos dados da solução;
h) A solução deve permitir a criação de, no mínimo, 20 contas para gerência e acesso aos relatórios, sem custo adicional;
i) 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).
34. Todas as licenças de uso de software devem ser registradas, na data da entrega, em nome da Contratante no site do fabricante.
35. Dos Relatórios:
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;
35.2. A solução deve possibilitar a criação de relatórios baseados na seleção de ativos, permitindo inclusive a seleção de todos os ativos existentes;
35.3. Deve suportar a criação de relatórios criptografados (protegidos por senha configurável) ;
35.4. A solução deve suportar o envio automático de relatórios para destinatários específicos;
35.5. Deve ser possível definir a frequência na geração dos relatórios para no mínimo: Diário, Mensal, Semanal e Anual;
35.6. Permitir especificar níveis de permissão nos relatórios para usuários e grupos específicos;
35.7. A solução deve fornecer relatórios do tipo “scorecard” para as partes interessadas da empresa;
35.8. A solução deve fornecer relatórios de correções aplicadas, classificados pelos seguintes critérios: grupo de ativos, usuários e vulnerabilidades;
36. A solução deve permitir mecanismo de varredura baseado em inferência com técnicas de varredura não intrusivas;
37. A solução deve possuir ou permitir a criação de relatórios com as seguintes informações:
37.1. Hosts verificados sem credenciais;
37.2. Top 100 Vulnerabilidades mais criticas;
37.3. Top 10 Hosts infectados por Malwares;
37.4. Hosts exploráveis por Malwares;

37.5. Total de vulnerabilidades que podem ser exploradas pelo Metasploit;
37.6. Vulnerabilidades críticas e exploráveis;
37.7. Máquinas com vulnerabilidades que podem ser exploradas;
38. A solução deve possuir dashboards customizáveis onde o administrador pode criar, editar ou remover painéis de acordo com a necessidade;
39. A solução deve ser capaz de inventariar todos os ativos da rede local e publicados na Internet, sem limites de endereços IPs.
40. A plataforma de software deve ser capaz de realizar varreduras (scans) de vulnerabilidades para no mínimo 250 IPs;
41. A plataforma de software deve ser licenciada para um número ilimitado de scanners (prevendo redundância);
42. Deve permitir a configuração de vários painéis e widgets;
43. Deve ser capaz de medir e reportar ameaças;
44. Deve ser capaz de visualizar ameaças críticas ao ambiente monitorado;
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;
46. A plataforma de software deve suportar vários mecanismos de varredura distribuídos em diferentes localidades e regiões e gerenciar todos por uma console central;
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;
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.
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.
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;
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;
52. A plataforma de software deve ser configurável para permitir a otimização das parametrizações de varredura;
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;
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;
55. A plataforma de software deve ser capaz de realizar pesquisas de dados confidenciais.
56. 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;

56.1. 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;
56.2. A solução de análise deve ser capaz de analisar, testar e reportar falhas de segurança em aplicações Web;
56.3. A solução de análise deverá ser capaz de executar varreduras em sistemas Web através de seus endereços IP ou FQDN (DNS);
56.4. A solução de análise deve ser capaz de identificar vulnerabilidades de divulgação de dados, como vazamento de informações de identificação pessoal;
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;
56.6. Deverá também permitir a execução da função crawler, que consiste na navegação para descoberta das URLs existentes na aplicação;
56.7. A solução de análise deve suportar a integração com o softwares de automação de testes para permitir sequências de autenticação complexas;
56.8. A solução de análise deve ser capaz de realizar testes/varreduras em aplicações separadas, simultaneamente limitadas ao número de licenças;
56.9. Suporte a ferramentas para construção de requisições e análise de respostas de aplicações WEB, API's e WebServices, tais como Postman Collections;
56.10. A solução de análise deve oferecer suporte à capacidade de testar novamente a vulnerabilidade específica que foi detectada anteriormente no aplicativo Web;
56.11. Deve ser capaz de utilizar scripts customizados de crawling com parâmetros definidos pelo usuário;
56.12. Deve ser capaz de excluir determinadas URLs da varredura através de expressões regulares;
56.13. Deve ser capaz de excluir determinados tipos de arquivos através de suas extensões;
56.14. 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;
56.15. Deve ser capaz de agendar a varredura e determinar sua frequência entre uma única vez, diária, semanal, mensal e anual;
56.16. Deve suportar o envio de notificações por email;
56.17. Deverá ser compatível com avaliação de web services REST e SOAP;
56.18. A solução de análise deve suportar os seguintes esquemas de autenticação:
a) Autenticação Básica (Digest);
b) NTLM;
c) Autenticação de Cookies;
56.19. Deve ser capaz de importar scripts de autenticação previamente configurados pelo usuário;
56.20. 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;
56.21. Os resultados devem ser apresentados agregados por vulnerabilidades ou por aplicações;
56.22. Para cada vulnerabilidade encontrada, deve ser exibido detalhes e evidências;
56.23. Cada vulnerabilidade encontrada deve conter também soluções propostas para mitigação ou remediação;
56.24. 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 e PDF.
57. 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.

Requisitos de Segurança
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 Mato Grosso do Sul aos quais tiver acesso em decorrência do objeto da presente contratação, ficando terminantemente proibida de fazer uso ou revelação destes sob qualquer justificativa;
2. O Tribunal Regional Eleitoral do Mato Grosso do Sul terá propriedade sobre todos os documentos e procedimentos operacionais produzidos no escopo da presente contratação;
3. Os documentos eventualmente produzidos deverão ser repassados ao Tribunal tanto em formato não editável (PDF) como também em formato editável (.DOCX).
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.

2.1.1 Soluções Disponíveis no Mercado de TIC (Art. 14, I, a)

- Solução utilizando 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.

- Solução paga com gerenciamento e armazenamento na nuvem (On Clound)
Nome da Solução: Ferramenta de Gestão de Vulnerabilidades On Clound
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 36 meses.

- 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 (0834081) e Rapid7 (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 36 meses ou de licença perpetua com suporte de 36 meses.

2.1.2 Contratações Públicas Similares (art. 14, I, b)

- Solução paga com gerenciamento e armazenamento na nuvem (On Clound)

Não foi encontrada contratação pública similar.

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

UASG 070019 - TRIBUNAL REGIONAL ELEITORAL DO PARANÁ - R$308.399,00

2.2 IDENTIFICAÇÃO DAS DIFERENTES SOLUÇÕES DE TIC (ART. 14, II)

2.2.1 Disponibilidade de STIC similar em outro órgão (Art. 14, II, a)

Foi procurado na Internet algum software desenvolvido por outro órgão e que atendesse às especificações solicitadas, porém nenhum foi encontrado.

2.2.2 STIC existente no Portal de Software Público Brasileiro (Art. 14, II, b)

Foi procurado no portal https://softwarepublico.gov.br/ algum software relativo às Soluções informadas, porém nenhum foi encontrado.

2.2.3 A capacidade e as alternativas do mercado de TIC (Art. 14, II, c)

Não se aplica, uma vez que não existe nenhum órgão público, de qualquer esfera, que forneça os softwares objetos deste estudo.

2.2.4 Observância ao Modelo Nacional de Interoperabilidade (Art. 14, II, d)

Não se aplica, uma vez que se trata de item relacionado a desenvolvimento de software e a solução aqui pretendida trata-se de solução de software.

2.2.5 Aderência às regulamentações da ICP-Brasil (Art. 14, II, e)

Não se aplica, uma vez que se trata de item relacionado a desenvolvimento de software e a solução aqui pretendida trata-se de soluções de software.

2.2.6 Observância ao Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Poder Judiciário (Moreq-Jus) (Art. 14, II, f)

Não se aplica, uma vez que se trata de item relacionado a desenvolvimento de software e a solução aqui pretendida trata-se de solução de segurança.

2.2.7 Orçamento estimado (Art. 14, II, g)

Item 1 - Solução de Segurança para Datacenter								
Subitem	Qtde	Descrição	Cloud (Nuvem) Rapid7	Cloud (Nuvem) Tenable	On premise (Local) Rapid7	On premise (Local) Tenable	On premise (Local) TRE-PR	Média dos valores (sem TRE-PR)
1.1	5 (licença)	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 pelo fabricante.	R$ 776.875,00	R$ 791.250,00	R$ 776.875,00	R$ 728.254,80	R$ 308.399,00	R$ 768.000,00
1.2	2 (licença)	Licenciamento para solução de análise dinâmica em aplicações Web, pacote para no mínimo 5 domínios (FQDN), por 36 meses de uso e suporte pelo fabricante.	R$ 493.200,00	R$ 129.420,00	R$ 739.860,00	R$ 0,00		R$ 454.160,00
1.3	1	Instalação e configuração da solução.	R$ 38.000,00	R$ 11.322,00	R$ 38.000,00	R$ 11.322,00		R$ 24.661,00
1.4	1	Repasse tecnológico, com período mínimo de 20 horas.	R$ 10.000,00	R$ 8.342,00	R$ 10.000,00	R$ 8.342,00		R$ 9.171,00
1.5	50	4 Horas de Serviço Especializado.	R$ 1.000,00	R$ 0,00	R$ 1.000,00	R$ 0,00		R$1.000,00
TOTAIS			R$ 1.319.075,00	R$ 940.334,00	R$ 1.565.735,00	R$ 747.918,80	R$ 308.399,00	R$ 1.256.992,00
VALOR TOTAL								R$ 165.000,00

Os orçamentos recebidos pelo TRE-PB e repassados para o TRE-MS, foram utilizados como base para dimensionar o orçamento estimado, mas ficaram muito acima do que foi previsto pela equipe de planejamento.

A contratação do TRE-PR foi extraída do Painel de Preços e possui mais licenças do que o TRE-MS pretende adquirir. Fizemos uma projeção com base nessa contratação, conforme tabelas abaixo:

Contratação TRE-PR

Item	Quantidade	Descrição	Valor Previsto	Valor Contr decréscimo para os it
1	9	~~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 pelo fabricante.	R$ 463.842,30	R$ 193
2	6	Licenciamento para solução de análise dinâmica em aplicações Web, pacote para no mínimo 10 domínios (FQDN), por 36 meses de uso e suporte pelo fabricante.	R$ 247.202,00	R$ 103
3	1	Instalação, Configuração e Treinamento de 16 horas	R$ 11.500,00	R$ 11.
VALOR TOTAL			R$ 722.544,30	R$ 308

Projeção para TRE-MS

Item	Quantidade	Descrição	Valor Previsto	Valor Contr decréscimo para os it
1	5	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 pelo fabricante.	R$ 257.690,20	R$ 107.
2	1	Licenciamento para solução de análise dinâmica em aplicações Web, pacote para no mínimo 10 domínios (FQDN), por 36 meses de uso e suporte pelo fabricante.	R$ 41.200,00	R$ 17.2
3	1	Instalação, Configuração e Treinamento de 16 horas	R$ 11.500,00	R$ 11.5
VALOR TOTAL			R$ 722.544,30	R$ 136.

A contratação do TRE-PR previu para o item 1, 9 licenciamentos para 250 IPs, o TRE-MS pretende apenas 5. Previu para o item 2, 6 licenciamentos para 10 domínios, o TRE-MS pretende dividir em 2 unidades, mas totalizando licenciamento para 10 domínios. O item 3, não entrou na diminuição dos valores porque é padrão. Sendo assim, fazendo um paralelo com a contratação recente do TRE-PR, o TRE-MS, realizaria uma despesa de aproximadamente R$136.302,90. Muito abaixo dos orçamentos recebidos.

Dessa forma, os orçamentos serão desconsiderados e o TRE-MS irá trabalhar com o orçamento previsto para a contratação, qual seja R$165.000,00.

2.3 ANÁLISE E COMPARAÇÃO ENTRE OS CUSTOS TOTAIS DAS STICs (ART. 14, III)

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.

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 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.

Solução 3 - Baseada em gerenciamento em rede local do tribunal (On premise) fornecida pela Tenable apresenta um valor de aquisição adequado e menor do que a Solução 2 (On clound). 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. Todos 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 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.

2.4 DA ESCOLHA E JUSTIFICATIVA DA STIC ESCOLHIDA (ART. 14, IV)

Sendo assim, dentre as alternativas avaliadas, no momento, a melhor solução para o TRE-MS é 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.

2.4.1 DESCRIÇÃO DA SOLUÇÃO (ART. 14 IV, A)

A solução de segurança deve possuir a seguinte característica:

Fornecimento de software, instalação, suporte, documentação e treinamento da Ferramenta de Gestão de Vulnerabilidades.

2.4.2 ALINHAMENTO DA SOLUÇÃO (ART. 14, IV, B)

A Solução escolhida atende às necessidades do Órgão quando contribui para atender às necessidades de TI, uma vez que melhora o indicador: “Segurança da informação, infraestrutura de processamento e aplicativos”, constante do PETI do TRE-MS.

2.4.3 BENEFÍCIOS ESPERADOS (ART. 14, IV, C)

- Atender requisito mínimo da resolução CNJ nº 211/2015 (Artigo 24, parágrafo VII);
- Garantir a proteção dos dados pessoais dos usuários através de: proteção contra ataques cibernéticos, tais como malwares e ramsonwares em servidores; inspeção de logs e monitoramento de integridade de arquivos e de bibliotecas utilizadas no desenvolvimento de aplicações do TRE-MS, conforme LGPD;

- Adquirir e implantar ferramenta de Gestão de Vulnerabilidades até dezembro/2020;
- Garantindo assim maior proteção aos dados hospedados no Datacenter do TRE-MS, sobretudo aos dados dos usuários.

2.4.4 RELAÇÃO ENTRE A DEMANDA PREVISTA E A SER CONTRATADA (ART. 14, IV, D)

A demanda prevista é a aquisição de Ferramenta de Gestão de Vulnerabilidades, bem como melhoria da segurança da informação.

A demanda a ser contratada é igual à quantidade prevista, e tem o intuito de apresentar solução definitiva ao problema apresentado neste estudo e implantá-la em tempo hábil.

2.5 ADEQUAÇÃO DO AMBIENTE (ART. 14, V, A, B, C, D, E, F)

Não será necessária nenhuma adequação do ambiente.

3 SUSTENTAÇÃO DO CONTRATO (ART. 15)

3.1 RECURSOS MATERIAIS E HUMANOS (ART. 15, I)

Todos os Recursos Materiais necessários para a implantação deverão ser fornecidos pela empresa contratada, conforme os requisitos listados no item 2.4.1.

Em relação aos Recursos Humanos, serão necessários:

- 02 (dois) servidores do quadro para atuarem como fiscais do contrato.

3.2 DESCONTINUIDADE DO FORNECIMENTO (ART. 15, II)

A descontinuidade do fornecimento de atualização irá causar impacto imediato na solução. Sendo necessária a aquisição/implantação de outro software que realize o mesmo papel dentro do TRE-MS.

3.3 TRANSIÇÃO CONTRATUAL (ART. 15, III, A, B, C, D, E)

Em caso de necessidade de transição contratual, será necessária a aquisição/implantação de novo software com funcionalidade igual ou superior.

3.4 ESTRATÉGIA DE INDEPENDÊNCIA TECNOLÓGICA (ART. 15, IV, A, B)

O TRE-MS possuirá independência tecnológica de operacionalização (haverá documentação de toda a solução e repasse de conhecimento).

4 ESTRATÉGIA PARA A CONTRATAÇÃO (ART. 16)

4.1 NATUREZA DO OBJETO (ART. 16, I)

Trata-se da aquisição de solução de software, o objeto pode ser fornecido por diversas revendas e possui características comuns e usuais no mercado de TIC, cujos padrões de desempenho e de qualidade estão objetivamente definidos.

4.2 PARCELAMENTO DO OBJETO (ART. 16, II)

Para esta aquisição não haverá parcelamento do objeto, pois o sucesso da implantação da Solução (uso integral de toda a potencialidade de aumento da segurança da Solução), depende de cada componente da Solução a ser adquirida, sejam eles componentes principais ou acessórios. Portanto, faz-se necessário o agrupamento para garantir o uso por completo do que venha a ser adquirido, evitando assim, que componentes da Solução venham a ser adquiridos e não utilizados (ou utilizados de forma precária).

4.3 ADJUDICAÇÃO DO OBJETO (ART. 16, III)

O objeto será licitado em item único, com subitens, portanto, a adjudicação será realizada somente para uma empresa fornecedora.

4.4 MODALIDADE E TIPO DE LICITAÇÃO (ART. 16, IV)

De início, esta Seção informa que a contratação se dará na modalidade de Pregão, nos termos da Lei 10.520/2002, uma vez que os materiais licitados podem ser enquadrados como bens comuns, nos termos do inciso II do art. 3º do Decreto nº 10.024/2019.

> *Art. 3º Para fins do disposto neste Decreto, considera-se:*
>
> ---

II - bens e serviços comuns - bens cujos padrões de desempenho e qualidade possam ser objetivamente definidos pelo edital, por meio de especificações reconhecidas e usuais do mercado;

Considerando a disposição contida no §1º do art. 1º do Decreto nº 10.024/2019, a licitação se dará na modalidade eletrônica:

Art. 1º Este Decreto regulamenta a licitação, na modalidade de pregão, na forma eletrônica, para a aquisição de bens e a contratação de serviços comuns, incluídos os serviços comuns de engenharia, e dispõe sobre o uso da dispensa eletrônica, no âmbito da administração pública federal.

§ 1º A utilização da modalidade de pregão, na forma eletrônica, pelos órgãos da administração pública federal direta, pelas autarquias, pelas fundações e pelos fundos especiais é obrigatória.

No que tange à escolha do **tipo** de licitação, por se tratar de serviços comuns, não resta outra opção a não ser o do tipo MENOR PREÇO.

Em atendimento ao disposto no cap. V da Lei Complementar 123/2006 alterada pela Lei Complementar 147/2014, observado o art. 8º do Decreto 7.174/2010 deverá ser observado as preferências na contratação (art. 3º da Lei 8.248/1991), explicitado no art. 5º a 8º do retromencionado diploma legal.

Com fulcro no Inciso IV do art. 49 da Lei 123/2006 e tendo em vista os motivos já expostos, não serão criadas as cotas de participação exclusiva. para as empresas ME/EPP.

Para a presente contratação, este TRE/MS poderá realizar um certame próprio ou, com o intuito de se obter "ganho" de escala, pela demanda agrupada de outros órgãos da Administração Pública, também mostra-se víavel apresentar-se com órgão partícipe de certame realizado por outro órgão.

4.5 CLASSIFICAÇÃO E INDICAÇÃO ORÇAMENTÁRIA (ART. 16,V)

As despesas decorrentes do objeto desta licitação, serão custeadas com recursos aprovados na Lei Orçamentária da União nº 13.978 de 20 de janeiro de 2020, que estima a receita e fixa a despesa da União para o exercício financeiro 2020 (LOA), Unidade 14112 – TRE-MS, Ação: 20GP– Julgamento de Causas e Gestão Administrativa, Programa de Trabalho: 02.122.0570.20GP.0054, Elementos de Despesa: 4490.40 - Aquisição de Softwares.

Este item poderá sofrer alteração pela COPEG, unidade responsável pela Informação quanto à reserva e enquadramento orçamentários para cobrir a despesa, e de sua compatibilização com a Lei Orçamentária Anual, Plano Plurianual e a Lei de Diretrizes Orçamentárias.

4.7 VIGÊNCIA DA PRESTAÇÃO DE SERVIÇO (ART. 16, VI)

O período de vigência desta contratação será de 36 (trinta e seis) meses, período de prestação de suporte on-site, contados da assinatura do contrato.

4.7 EQUIPE DE APOIO À CONTRATAÇÃO (ART. 16, VII)

Sugestão da equipe de apoio e fiscais do contrato:

- Gustavo Leite Pinho (Titular)
- Alexandre Arashiro Oyakawa (Substituto)

4.8 EQUIPE DE GESTÃO DA CONTRATAÇÃO (ART. 16, VIII)

As atribuições cabíveis à fiscalização administrativa podem ser desempenhadas pela fiscalização técnica, auxiliada, no que couber, pela Seção de Gestão de Contratos Administrativos.

5 ANÁLISE DE RISCOS

RISCO 1 - Licitação deserta			
Probabilidade	ID	Dano	Impacto
Média	1	Não realizar a contração	Médio
ID	Ação de Mitigação e Contingência		Responsável
1 - Mitigação	Solicitar a realização de nova licitação ou Dispensa nos mesmos moldes do edital.		Gustavo Pinho

6 DECLARAÇÃO DA VIABILIDADE DA CONTRATAÇÃO

A equipe de planejamento, diante dos dados expostos, entende que a contratação é viável e necessária, aumentando assim, a partir de sua implantação, a segurança das informações armazenadas e disponibilizadas pelo TRE-MS.

Documento assinado eletronicamente por **MARIA JULIA DE ARRUDA MESTIERI**, **Analista Judiciário**, em 23/10/2020, às 13:26, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **GUSTAVO LEITE PINHO**, **Técnico Judiciário**, em 23/10/2020, às 16:07, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://sei.tre-ms.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0913367** e o código CRC **99657EFA**.

0007346-21.2020.6.12.8000 0913367v21

JUSTIÇA ELEITORAL
TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO SUL

Administração - Aquisição - Bens de Consumo - 0009384-54.2020.6.21.8000
Estudos Técnicos Preliminares - ETP - doc. SEI n. 0447443.

CONTRATAÇÃO DE TIC **ANÁLISE DE RISCOS**			
Solução de TIC a ser contratada: Solução para Avaliação de Vulnerabilidades em Ativos de Informação e para Avaliação Dinâmica de Aplicações WEB			
RISCOS			
Descrição do risco:	Descontinuação do produto	Vazamento de dados sobre vulnerabilidades	Não conseguir finalizar a contratação este ano
Tipo:	(X) Risco da Solução de TIC ( ) Risco do Processo de Contratação	(X) Risco da Solução de TIC ( ) Risco do Processo de Contratação	(X) Risco da Solução de TIC ( ) Risco do Processo de Contratação
Probabilidade:	(X) Baixa ( ) Média ( ) Alta	(X) Baixa ( ) Média ( ) Alta	( ) Baixa (X) Média ( ) Alta
Dano Potencial:	Ficar sem as atualizações sobre vulnerabilidades (principal valor agregado da solução) ou sem acesso à solução.	Atacantes teriam informações privilegiadas que facilitariam um ataque contra a infraestrutura de TIC	Não contratar a solução e não executar a verba alocada para essa contratação
Ação Preventiva e Responsável:	Prever essa situação em contrato – Equipe de contratação	Solicitar selos de segurança que garantam melhores controles de segurança para minimizar a probabilidade da ocorrência de vazamentos – Equipe de contratação	Agilizar o processo de contratação – Todos envolvidos no processo de contratação

Ação de Contingência e Responsável:	Providenciar a contratação de outra solução - STI	Ao tomar conhecimento de um vazamento, realizar uma força-tarefa para identificar sistemas que tenham sido comprometidos e implementar medidas de controle para que as vulnerabilidades vazadas não possam ser exploradas - SEGTI	Alinhar a contratação para o próximo ano e redirecionar a verba para outra contratação - STI

Equipe de Planejamento da Contratação
Márcio Barbosa de Carvalho Integrante demandante
Rodrigo Bueno Cantini Integrante técnico
José Atílio Benites Lopes Integrante administrativo

Documento assinado eletronicamente por **Rodrigo Bueno Cantini**, **Técnico Judiciário**, em 08/10/2020, às 13:02, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Marcio Barbosa de Carvalho**, **Técnico Judiciário**, em 13/10/2020, às 18:57, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-rs.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0447443** e o código CRC **B7138B84**.

JUSTIÇA ELEITORAL
TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO SUL

DOCUMENTO DE OFICIALIZAÇÃO DE DEMANDA - DOD
Resumo do objeto da demanda: Necessidade de ferramenta para gestão de vulnerabilidades dos ativos de informação do TRE-RS.

IDENTIFICAÇÃO DA ÁREA DEMANDANTE	
Unidade/Setor:	STI/COINF
Responsável:	Mateus Vicente Marchi
Integrante Demandante Indicado:	Márcio Barbosa Carvalho

NECESSIDADE DE MOTIVAÇÃO DA SOLICITAÇÃO

Como resultado de uma avaliação recente junto ao Gartner, empresa de aconselhamento contratada pelo TRE-RS, foram identificadas e priorizadas ações necessárias para elevar nossa maturidade de Segurança da Informação. Entre essas ações foram priorizadas, entre outras, a gestão de vulnerabilidades e a gestão de eventos de segurança da informação. Em complementação aos resultados dessa avaliação do Gartner, também foram feitas priorizações de ações recomendadas por um reconhecido *framework* de Segurança da Informação chamado CIS Controls (Center of Internet Security). Esse *framework* também recomenda controles de segurança relacionados à gestão de vulnerabilidades e de eventos de segurança da informação para organizações do porte do TRE-RS.

Para a gestão de eventos de segurança da informação, o TRE-RS adquiriu no final de 2019 (processo SEI 0004824-06.2019.6.21.8000) uma solução de SIEM (*Security Information and Event Management)* da IBM, chamada QRadar, cuja primeira fase de implementação, com o auxílio da contratada (Teletex), foi concluída no mês de março de 2020.

A gestão de vulnerabilidades é um processo complementar ao de gestão de eventos de segurança da informação realizado pelo SIEM. Esse processo preocupa-se com a descoberta e remediação de vulnerabilidades que podem estar presentes nos sistemas de informação. Uma vulnerabilidade pode surgir pela utilização de uma versão comprometida de um software ou por uma configuração inadequada desse software. Essa vulnerabilidade pode ser explorada por um atacante para prejudicar a disponibilidade, integridade e confidencialidade dos ativos de informação. Devido à complexidade e quantidade de ativos de informação utilizados no nosso ambiente de TIC, o processo de gestão de vulnerabilidades necessita ser suportado por uma solução de gestão de vulnerabilidades. Essa solução deverá monitorar os ativos de informação da infraestrutura de TIC do TRE e apontar suas vulnerabilidades, suportando o processo de gestão de vulnerabilidades e gerando incidentes de segurança no IBM Qradar.

Desta forma, solicitamos a aquisição de solução para gestão de vulnerabilidades, na modalidade de serviço ou então com subscrição mínima de 60 meses. Esta solução poderá ser contratada através de aquisição do módulo de gestão de vulnerabilidades do IBM QRadar, através de licenciamento adicional. Porém, há no mercado soluções de outros fabricantes que se integram ao IBM Qradar, e que, portanto, deverão ser avaliadas.

O custo estimado para utilização desta ferramenta foi estimado em R$120.000,00 por ano , quando da elaboração de plano de contratação de 2020.

RESULTADOS A SEREM ALCANÇADOS

- Identificação das vulnerabilidades das soluções de TIC utilizadas pelo TRE-RS.
- Redução do nível de risco através da redução da probabilidade de ameaças explorarem as vulnerabilidades de nossos ativos;

- Aderência do TRE-RS às boas práticas aconselhadas pelo Gartner e definidas na CIS Controls (Center of Internet Security);

SUGESTÃO DE SOLUÇÃO (não vincula os estudos)
Aquisição de software para Gestão de Vulnerabilidades que se integre ao SIEM(Sistema de Gestão de Informações e Eventos de Segurança da Informação) to TRE-RS, IBM Qradar.

ALINHAMENTO ESTRATÉGICO

A solicitação está alinhada a algum objetivo do planejamento estratégico institucional do Tribunal?

[X] **Sim - Qual?**

[ ] 1. Assegurar a legitimidade e o aprimoramento do processo eleitoral
[ ] 2. Promover a efetiva prestação jurisdicional
[ ] 3. Fomentar a aproximação da Justiça Eleitoral com a sociedade
[ ] 4. Aperfeiçoar a governança institucional
[X] 5. Buscar a excelência na gestão
[ ] 6. Promover a responsabilidade socioambiental e a acessibilidade na Justiça Eleitoral
[ ] 7. Aprimorar a comunicação interna
[ ] 8. Fortalecer o engajamento de servidores e colaboradores
[ ] 9. Desenvolver pessoas por competências
[X] 10. Aperfeiçoar a infraestrutura de TI
[ ] 11. Aperfeiçoar a infraestrutura física
[ ] 12. Aperfeiçoar a gestão orçamentária
[ ] **Não.**

A contratação está alinhada a algum objetivo do planejamento estratégico de TI?

[X] **Sim - Qual?**

[ ] 1. Atender à ENTIC-JUD.
[ ] 2. Garantir o cumprimento do PDTIC.
[ ] 3. Executar processo de TIC conforme boas práticas.
[ ] 4. Consolidar o gerenciamento de projetos
[ ] 5. Aprimorar as contratações de TIC.
[X] 6. Aprimorar a gestão de riscos de TIC
[X] 7. Garantir a disponibilidade da infraestrutura de TIC.
[ ] 8. Aprimorar competências da STI.
[ ] 9. Otimizar o orçamento de TIC.
[ ] **Não.**

ÁREA DEMANDANTE DA SOLUÇÃO

MATEUS VICENTE MARCHI
STI/COINF

Obs.: o Documento de Oficialização de Demanda - DOD deverá ser assinado pelo responsável pela demanda.

Documento assinado eletronicamente por **Mateus Vicente Marchi**, **Coordenador**, em 25/05/2020, às 10:50, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-rs.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0312577** e o código CRC **62855FE4**.

Avenida Padre Cacique, 96 - Bairro Praia de Belas - Porto Alegre/RS - CEP 90810-240
www.tre-rs.jus.br - Fone: (51) 3294 8399

JUSTIÇA ELEITORAL
TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO SUL

Administração - Aquisição - Bens de Consumo - 0009384-54.2020.6.21.8000
Estudos Técnicos Preliminares - ETP - doc. SEI n. 0445040.

CONTRATAÇÃO DE TI

PLANO DE SUSTENTAÇÃO DO CONTRATO

Solução de TI a ser contratada: Solução para Avaliação de Vulnerabilidades em Ativos de Informação e para Avaliação Dinâmica de Aplicações WEB

RECURSOS A SEREM PROVIDOS PELO TRIBUNAL

Descrição	Material/Humano	Próprio / A ser contratado	Área Responsável
Acompanhamento técnico para instalação e configuração inicial da solução	02 servidores	Próprio	SEGTI/SERBA

ESTRATÉGIA DE CONTINUIDADE EM EVENTUAL INTERRUPÇÃO CONTRATUAL

Em caso de interrupção contratual, descreva como serão afetados os serviços prestados pelo Tribunal:

Caso a solução seja interrompida, o TRE-RS ficará sem as avaliações de vulnerabilidades. Portanto, novas vulnerabilidades não serão encontradas. Entretanto, como boa parte do tempo dedicado ao processo de gestão de vulnerabilidades é dedicado às remediações, as equipes de TIC podem utilizar os relatórios emitidos pela solução enquanto estava em funcionamento para continuar as remediações até que a solução seja restabelecida ou outra solução seja contratada.

Ações de contingência e seus respectivos responsáveis:

Os relatórios deverão ser salvos rotineiramente tanto para documentação como para continuidade do processo de remediação no caso de descontinuidade do contrato.

Responsáveis: Essa ação ficará a cargo da SEGTI.

TRANSIÇÃO E ENCERRAMENTO CONTRATUAL		
(x) **Serviços**	Com que **antecedência** o gestor do contrato deverá analisar a possibilidade e o interesse da administração na **prorrogação** do contrato **ou** na eventual condução de uma **nova contratação**?	6 meses
	No caso de uma nova contratação, qual o **tempo necessário de sobreposição contratual** a fim de viabilizar a transferência de conhecimento, sem prejuízos ao Tribunal?	
( ) **Equipamentos**	Com que **antecedência** o gestor do contrato deverá analisar a necessidade e conveniência da contratação de serviços de **manutenção ou** da **substituição dos equipamentos**, de acordo com o critério vigente no Tribunal em relação à manutenção e atualização do parque de equipamentos?	

Ações Necessárias no Encerramento Contratual	**Responsável**	**Prazo**
( ) Entrega de versões finais dos produtos		
( ) Transferência final de conhecimentos sobre a execução e a manutenção da solução de TI		
( ) Devolução de recursos materiais		
(x) Revogação de perfis de acesso	SEGTI	1 mês após o término
( ) Eliminação de caixas postais		
(x) Outras: Backup dos dados disponíveis na solução, bem como relatórios, para documentação e continuidade do processo de remediação até que nova solução seja implantada.	SEGTI	Antes da data de encerramento do contrato/vigência das licenças

ESTRATÉGIA DE INDEPENDÊNCIA DA ADMINISTRAÇÃO	
(x) **Transferência de Conhecimento**	A transferência de conhecimento se dará através de acompanhamento dos serviços de instalação e configuração.

( ) **Direitos de Propriedade Intelectual e Direitos Autorais**	Pertencerão exclusivamente ao Tribunal os direitos relativos aos produtos desenvolvidos e elaborados para a prestação do objeto, sendo vedada sua reprodução, transmissão e/ou divulgação sem o seu respectivo consentimento.

SEGURANÇA DA INFORMAÇÃO E CONTROLE DE ACESSO
(x) Durante a prestação do objeto, a Contratada deverá observar as Políticas de Controle de Acesso definidas pelo Tribunal.
(x) A contratada deverá firmar Termo de Compromisso com a Segurança da Informação conforme minuta em anexo.

Equipe de Planejamento da Contratação
Márcio Barbosa de Carvalho Integrante demandante
Rodrigo Bueno Cantini Integrante técnico
José Atílio Benites Lopes Integrante administrativo

Documento assinado eletronicamente por **Rodrigo Bueno Cantini**, **Técnico Judiciário**, em 08/10/2020, às 13:02, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Marcio Barbosa de Carvalho**, **Técnico Judiciário**, em 13/10/2020, às 18:56, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-rs.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0445040** e o código CRC **25B89B38**.

Avenida Padre Cacique, 96 - Bairro Praia de Belas - Porto Alegre/RS - CEP 90810-240
www.tre-rs.jus.br - Fone: 3294 8404

JUSTIÇA ELEITORAL
TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO SUL

Administração - Aquisição - Bens de Consumo - 0009384-54.2020.6.21.8000
Estudos Técnicos Preliminares - ETP - doc. SEI n. 0444604.

CONTRATAÇÃO DE TI

ANÁLISE DE VIABILIDADE TÉCNICA DA CONTRATAÇÃO

Solução de TI a ser contratada: Solução para Avaliação de Vulnerabilidades em Ativos de Informação e para Avaliação Dinâmica de Aplicações WEB

DEFINIÇÃO E ESPECIFICAÇÃO DOS REQUISITOS DA CONTRATAÇÃO DEFINIÇÃO E ESPECIFICAÇÃO DOS REQUISITOS DA CONTRATAÇÃO

Requisitos de Negócio	Justificativa
Solução para avaliação de vulnerabilidades de softwares para complementar a solução de gerenciamento de informações e eventos de segurança (SIEM) instalada no início de 2020.	Uma vulnerabilidade pode surgir pela utilização de uma versão comprometida de um software ou por uma configuração inadequada desse software. A exploração de uma vulnerabilidade por um atacante pode prejudicar a disponibilidade, integridade e confidencialidade dos ativos de informação. Portanto, elas são uma grande fonte de ameaças para sistemas e informações sensíveis. Devido à complexidade e quantidade de ativos de informação utilizados no ambiente de TIC do TRE-RS, o processo de gestão de vulnerabilidades necessita ser suportado por uma solução de avaliação de vulnerabilidades. Essa solução deverá monitorar os ativos da infraestrutura de TIC e apontar suas vulnerabilidades, suportando o processo de gestão de vulnerabilidades e enriquecendo as informações e eventos de segurança gerenciados pela solução de SIEM (IBM Qradar) instalada em 2020.
Principais Requisitos Tecnológicos	**Justificativa**
Escaneamento de vulnerabilidades: ativo, com e sem a utilização de agentes, autenticado e não-autenticado.	- ativo: realizado através de testes de conexão diretamente direcionados aos serviços disponíveis nos ativos monitorados. Em contraste ao escaneamento passivo, em que uma solução analisa o tráfego regular entre usuários e estes serviços, porém exigindo capacidades de replicação de tráfego para que este chegue à solução. Essa capacidade de replicação necessita de suporte da infraestrutura de rede, que não está disponível em todos os ambientes de TIC que estão no escopo desta contratação. - com e sem agente: em alguns ativos da infraestrutura de TIC não é possível instalar agentes, portanto a solução deve suportar escaneamento sem a necessidade de agentes. Por outro lado, esses agentes melhoram a capacidade de detecção de vulnerabilidades, pois por serem instalados nos ativos têm acesso a mais informações sobre os softwares instalados. Portanto, a solução deve suportar escaneamento com e sem a utilização de agentes. - autenticado e não-autenticado: autenticado para aumentar a capacidade de descoberta de vulnerabilidades, pois com acesso interno ao ativo é possível apontar vulnerabilidades em softwares que não atuam como serviços (sem a abertura portas de transporte em escuta). Tal como ocorre em relação a agentes, em alguns ativos não é possível realizar escaneamento autenticado, nesse caso a solução pode inspecionar externamente os serviços disponibilizados por este ativo. Portanto, a solução deve suportar escaneamento autenticado e não-autenticado.
Processo de priorização de vulnerabilidades baseado no risco de exploração que possa ser ajustado ao ambiente de TIC do TRE-RS.	É comum que soluções de avaliação de vulnerabilidades utilizem a métrica CVSS (*Common Vulnerability Scoring System*) para a priorização das vulnerabilidades que devem ser remediadas. Entretanto, essa métrica é aferida para ambientes computacionais em geral e não considera aspectos relacionados à importância do ativo ou software para o ambiente de TIC do TRE-RS. Nesse sentido, a remediação de vulnerabilidades em softwares que suportam ativos de informação mais críticos ou mais expostos devem ser priorizadas. A solução deve permitir que sejam informados níveis de criticidade para os ativos monitorados para uma priorização mais adequada.

Avaliação de segurança de configurações dos ativos conforme orientações dos fornecedores de software	Os fornecedores de software divulgam recomendações de segurança acerca da configuração de seus produtos. Configurações inadequadas podem ser exploradas por atacantes e serem tão danosas quanto a instalação de um software vulnerável.
Modelo de entrega SaaS (*Software as a Service*)	Durante os estudos, percebeu-se que os fornecedores entregam mais funcionalidades na modalidade SaaS. Além disso, a manutenção do ambiente da solução é realizada pela própria fabricante, reduzindo os custos operacionais do TRE-RS, que incluiriam equipe dedicada a dar manutenção na plataforma e a infraestrutura computacional necessária para suportar a solução. Tanto equipes quanto infraestrutura são recursos escassos, então opta-se pela solução no modelo SaaS.
Identificação de novos ativos conectados à rede	Novos ativos conectados à rede requerem atenção especial em relação a aspectos de segurança. Precisa-se saber se o surgimento de tal ativo era esperado ou trata-se de um ativo não autorizado. Além disso, novos ativos podem exigir avaliações mais rigorosas para assegurar que não introduzem vulnerabilidades na rede.
Integração nativa com o IBM QRadar SIEM	O TRE-RS realizou um investimento importante em uma solução de SIEM, que pode ser bastante enriquecida com informações sobre vulnerabilidades. Nesse sentido, com essas informações, uma ofensa detectada pelo SIEM pode ser melhor avaliada e priorizada, pois seu contexto será complementado com a existência de vulnerabilidades nos ativos envolvidos na ofensa.
Atualizações da base de vulnerabilidades, ameaças e recomendações de tratamento (remediações, mitigação e aceitação)	O valor agregado da solução está diretamente relacionado à qualidade das informações sobre as vulnerabilidades, recomendações e seus tratamentos. Essas informações devem ser atualizadas constantemente.
Capacidade de redução das vulnerabilidades identificadas	Uma parte considerável do esforço no processo de gestão de vulnerabilidades é dedicado a analisar e priorizar as vulnerabilidades para decidir o tratamento adequado. Ao reduzir automaticamente o número de falsos positivos e vulnerabilidades duplicadas, a solução ajuda na eficiência do processo de gestão de vulnerabilidades.
Interface de gerenciamento centralizada	Essencial para uma visão panorâmica e sistemática de todo parque computacional em relação às vulnerabilidades a serem avaliadas. Em contraste a soluções em que as vulnerabilidades são visualizadas em uma interface dedicada a apenas um ativo.
Base de dados de ativos incorporada à solução	A solução não pode depender de um CMDB (*Configuration Management Database*) de mercado, pois não o possuímos. Portanto, a solução deve ter uma base de dados de ativos incorporada à solução.
Suporte a banco de dados Oracle	A solução deve ser capaz de inspecionar configurações destes bancos de dados sob o ponto de vista de recomendações de segurança.
Avaliação dinâmica de aplicações	Muitas das aplicações utilizadas no TRE-RS foram desenvolvidas internamente pela STI, pelo TSE ou por terceiros. Por serem de finalidade específica e não serem públicas, essas aplicações não são avaliadas pelas empresas que mantém bases de dados sobre vulnerabilidades. Por outro lado, essas aplicações são tão (ou mais) sensíveis que softwares de uso geral e podem conter vulnerabilidades em sua programação. Para avaliar a programação dessas aplicações, é necessária a utilização de uma solução de avaliação dinâmica, que consiste em expor a aplicação a tentativas de exploração (por exemplo, SQL injection, cross-site scripting (XSS)) que seriam utilizadas por um atacante, afim de detectar se são suscetíveis a essas técnicas de exploração.

CONSULTAS E ESTUDOS REALIZADOS

- **Nessus Professional.** Foi realizado um teste com a versão de avaliação oferecida diretamente no site do fabricante. Entretanto, verificou-se que a API que permitia sua integração com o IBM Qradar SIEM foi descontinuada a partir da versão 7 (atualmente o software está na versão 8).
- **Trend Micro Deep Security através da empresa PBI.** Foi realizado um teste da solução. Ela não oferece funcionalidades para a gestão das vulnerabilidades (priorização daquelas cujo risco é elevado). Por outro lado, ela oferece remediação automática (Virtual Patching) das vulnerabilidades identificadas. A remediação por virtual patching é considerada uma solução para vulnerabilidades em softwares que são difíceis ou impossíveis (limitação de atualização por falta de licenciamento adequado) de serem atualizados. Portanto, essa solução pode ser interessante para aquisição futura, pois ao executar o processo de gestão de vulnerabilidades poderemos identificar vulnerabilidades em softwares que não poderemos atualizar. Nesse caso, poderemos utilizar a solução de virtual patching para remediar a vulnerabilidade.
- **OpenVAS** (https://www.openvas.org/). É uma solução baseada em software livre para realizar avaliações de vulnerabilidades. Entretanto, desde 4 de setembro de 2017, sua base de dados de vulnerabilidades (*Greenbone Community Feed*) não recebe novos testes direcionados a softwares utilizados em ambientes corporativos. A partir dessa data, esses testes são incluídos apenas na versão comercial de sua base (*Greenbone Security Feed*), que não é possível adquirir à parte. Portanto, o OpenVAS não é uma solução adequada para o ambiente corporativo do TRE-RS.
- **Outpost24 através da empresa Brasoftware.**
- **Módulo Vulnerability Management for IBM Qradar SIEM através da empresa Teletex.**
- **Tenable.io (on cloud) e Tenable.sc (on premises) através da empresa Servix.**
- **Qualys VMDR através da empresa Service IT.**

IDENTIFICAÇÃO DAS DIFERENTES SOLUÇÕES

Solução 1:	Solução de avaliação de vulnerabilidades (Qualys VM) e avaliação dinâmica de aplicações (Qualys WAS) hospedada em nuvem no modelo SaaS.			
Valor Estimado:	Qualys VM para 500 IPs monitorados por 5 anos = R$ 220.000,00 (contratação TRE-PR em abril/2020) Qualys WAS para 10 FQDNs monitorados por 5 anos = R$ 84.500,00 (contratação TRE-PR em abril/2020)			
Informações Adicionais:	Implantada em outro órgão?	Sim (TRE-PR)	Aderente MNI (Modelo Nacional de Interoperabilidade)?	Não
	Software livre ou software público?	Não	Aderente à ICP-Brasil?	Não
	Disponível no Portal do Software Público?	Não	Aderente à Moreq-Jus?	Não
Solução 2:	Solução de avaliação de vulnerabilidades (Tenable.sc) com Web Application Scanning oferecida on-premises.			
Valor Estimado:	Tenable.sc para 500 Ips monitorados por 5 anos = R$ 213.890,63 (Proposta Comercial ServixIT) Tenable Web Application Scanning para 10 FQDNs monitorados por 5 anos = R$ 0,00 (incluída na licença acima - Proposta Comercial ServixIT).			
Informações Adicionais:	Implantada em outro órgão?	Não	Aderente MNI (Modelo Nacional de Interoperabilidade)?	Não
	Software livre ou software público?	Não	Aderente à ICP-Brasil?	Não
	Disponível no Portal do Software Público?	Não	Aderente à Moreq-Jus?	Não

ANÁLISE E COMPARAÇÃO ENTRE OS CUSTOS DAS SOLUÇÕES DE TI

Embora a solução no modelo SaaS seja mais cara do que a solução no modelo on-premises, há de se considerar que o TRE-RS não precisaria arcar com o custo operacional e da infraestrutura computacional no modelo SaaS. Portanto, o custo da solução em nuvem está adequado e competitivo em relação ao modelo on premises.

SOLUÇÃO ESCOLHIDA

Solução:	Solução 1 no modelo SaaS. Além dos itens listados nas soluções, há previsão de custo de instalação, treinamento e horas de serviço especializado independentemente da solução escolhida que está estimado em R$ 11.390,00 para instalação e treinamento e de R$ 12.500,00 para 40 horas de serviço especializado (10 blocos de 4 horas a serem registrados).
Justificativa:	**a) Alinhamento em relação às necessidades de negócio e requisitos tecnológicos:** Ambas soluções atendem os requisitos de negócio e tecnológicos. **b) Identificação dos benefícios a serem alcançados com a solução escolhida em termos de eficácia, eficiência, economicidade e padronização:** A solução em nuvem oferece a vantagem de não requerer a disponibilização de recursos computacionais da infraestrutura de TIC do TRE-RS. Além disso, parte da gerência da solução (atualização, instalação de patches) é realizada pela contratada. A diferença de custo entre as duas soluções justifica esses benefícios.

	c**) Relação entre a demanda prevista e a quantidade dos bens e/ou serviços a serem contratados:** A equipe realizou uma estimativa de que são necessárias 500 licenças para avaliação de vulnerabilidades e serão registradas mais 128 licenças para eventual crescimento. Quanto às aplicações, estima-se que 10 aplicações possam ser objeto de análise simultaneamente e serão registradas mais 5 licenças para eventual crescimento.

NECESSIDADES DE ADEQUAÇÃO DO AMBIENTE PARA EXECUÇÃO CONTRATUAL

a) infraestrutura tecnológica:

será necessária a instalação de uma máquina virtual para atuar como agente de escaneamento. Trata-se de uma máquina virtual de pequeno porte (1 CPU, 2GB de RAM, 50 IOPs) facilmente provisionada no nosso ambiente de TIC.

b) infraestrutura elétrica:

Não necessita alteração de infraestrutura elétrica.

c) logística de implantação:

Simples

d) espaço físico:

Não necessita alteração de espaço físico.

e) mobiliário:

Não necessita alteração de mobiliário.

f) impacto ambiental:

Não haverá impacto ambiental

Equipe de Planejamento da Contratação

Márcio Barbosa de Carvalho

Integrante Demandante

Rodrigo Bueno Cantini

Integrante Técnico

José Atílio Benites Lopes

Integrante Administrativo

Documento assinado eletronicamente por **Rodrigo Bueno Cantini**, **Técnico Judiciário**, em 08/10/2020, às 13:02, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Marcio Barbosa de Carvalho**, **Técnico Judiciário**, em 13/10/2020, às 18:56, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-rs.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0444604** e o código CRC **226AA5EE**.

Avenida Padre Cacique, 96 - Bairro Praia de Belas - Porto Alegre/RS - CEP 90810-240
www.tre-rs.jus.br - Fone: 3294 8404

JUSTIÇA ELEITORAL
TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO SUL

Administração - Aquisição - Bens de Consumo - 0009384-54.2020.6.21.8000
Estudos Técnicos Preliminares - ETP - doc. SEI n. 0447291.

CONTRATAÇÃO DE TI

ESTRATÉGIA PARA A CONTRATAÇÃO

Solução de TIC a ser contratada: Solução para Avaliação de Vulnerabilidades de Softwares e para Avaliação Dinâmica de Aplicações WEB

NATUREZA DO OBJETO

(X) O objeto pretendido é de natureza comum no âmbito do mercado de tecnologia da informação.

( ) Outra:

DETALHAMENTO DOS BENS E SERVIÇOS QUE COMPÕEM A SOLUÇÃO

Lote	Item	Descrição	Classif. Orçamentária	SIASG	Unidade	Quantidade Estimada	Justificativa da Quantidade
1	1	Licença da solução de avaliação de vulnerabilidades por endereço IP ou ativo por 5 anos	AQISOF	27464	Unidade	628	As licenças são ofertadas em pacotes de 500, 250 ou 128 IPs monitorados, sendo que pacotes maiores oferecem preço mais vantajoso por licença. Foram contabilizados em torno de 500 ativos a serem monitorados. Foram adicionadas 128 licenças para eventual crescimento do ambiente.
	2	Licença da solução de avaliação dinâmica de aplicações por FQDN (*Full Qualified Domain Name*) por 5 anos	AQISOF	27464	Unidade	15	As aplicações são avaliadas apenas em determinados momentos de seu ciclo de vida (por exemplo, atualização de versão, nova funcionalidade, implantação de solução de terceiro). Portanto, o número de licenças necessárias é proporcional à capacidade de desenvolvimento e implantação por parte da equipe da COSIS. Estima-se que 10 aplicações estejam sendo alteradas ou implantadas pela COSIS concomitantemente. Foram adicionadas 5 licenças para eventual crescimento do ambiente.
	3	Serviço de instalação	AOSI APOIO	26972	Unidade	1	Esse serviço é utilizado apenas na implantação da solução.
	4	Treinamento de 20 horas	AOSI APOIO	3840	Unidade	4	2 servidores da SEGTI e 2 da SERBA
	5	Bloco de 4 horas de serviço especializado	AOSI APOIO	26972	Unidade	10	Horas de serviço a serem utilizadas para dirimir dúvidas, solicitar consultoria e resolução de problemas de configuração que estejam fora do escopo do suporte oferecido pelo fabricante.

PARCELAMENTO DO OBJETO

( ) Parcelado. O objeto pode ser adjudicado a uma ou várias empresas, por itens.

(x) Agrupado em lotes. O objeto deverá ser adjudicado por lotes de itens.

Justificativa:

As vulnerabilidades identificadas pelos itens 1 e 2 deverão ser priorizadas seguindo um mesmo processo de tratamento que leva em consideração as capacidades de remediação das equipes de TIC. Portanto, como serão tratadas pelo mesmo processo, é necessário que estejam em uma mesma solução. Além disso, ao se identificar um conjunto de vulnerabilidades em um ativo (identificadas tanto pelo item 1 ou pelo item 2) pode-se chegar a conclusão que uma remediação mais abrangente seja mais adequada. A visão dessas vulnerabilidades em uma solução única facilita o planejamento de remediações atinentes a um mesmo ativo.
Os itens 3, 4 e 5 são referentes ao que for entregue nos itens 1 e 2, por esse motivo fazem parte do mesmo lote.

FORMA DE SELEÇÃO DO FORNECEDOR

(MODALIDADE E TIPO DE LICITAÇÃO)

Forma de Contratação:	**Justificativa:**
( ) Pregão Eletrônico **(x)** Pregão Eletrônico com Registro de Preços **( )** Adesão à Ata de Registro de Preços **( )** Inexigibilidade de Licitação **( )** Dispensa de Licitação **(x)** Outra: Pregão Eletrônico com Registro de Preços em conjunto com TSE e outros TREs	As quantidades de licenças a serem adquiridas para os itens 1 e 2 devem acompanhar a quantidade de ativos instalados no parque computacional do TRE-RS. Portanto, o registro de preços é a opção adequada para poder adquirir licenças no caso de aumento da quantidade de ativos no parque computacional. Os preços ofertados para as licenças é inversamente proporcional às quantidades a serem adquiridas. Nesse sentido, há um esforço conjunto do TSE e outros TREs para lançar uma ata de registro de preços conjunta, afim de aumentar a quantidade de licenças a serem registradas globalmente e consequentemente reduzir o preço das licenças individualmente.

VIGÊNCIA

(x) Vigência da ata de RP (em meses):	12 meses
(X) Vigência do contrato (em meses):	Itens 1 e 2: 60 meses
( ) Prazo de garantia (em meses):	

Justificativas: A solução a ser adquirida será utilizada em conjunto com a solução de SIEM implantada este ano. A solução de SIEM tem suporte e garantia por 60 meses. Nesse sentido, já que alguns requisitos técnicos desta solução estão atrelados ao SIEM, faz sentido que essa contratação acompanhe o período da contratação do SIEM.

EQUIPE DE GESTÃO DA CONTRATAÇÃO

	Titular	**Substituto**
(X) Gestor	Rodrigo Cantini	Mara Lange

(X) Fiscal Técnico	Márcio Barbosa de Carvalho	Ivo Antonio Guimarães Netto
( ) Fiscal Demandante		
( ) Fiscal Administrativo		

CARACTERIZAÇÃO DE SERVIÇOS CONTINUADOS

O objeto da contratação se estende necessariamente por mais de um ano?	**(x) Sim** **( ) Não**	**Justificativa:** A solução a ser adquirida será utilizada em conjunto com a solução de SIEM implantada este ano. A solução de SIEM tem suporte e garantia por 60 meses. Nesse sentido, já que alguns requisitos técnicos desta solução estão atrelados ao SIEM, faz sentido que essa contratação acompanhe o período da contratação do SIEM.
O objeto da contratação é essencial para a continuidade do negócio?	**( ) Sim** **(x) Não**	**Justificativa:** Sem a solução, não poderemos identificar novas vulnerabilidades. Entretanto, poderemos continuar a remediação das vulnerabilidades identificadas enquanto a solução estava em funcionamento. A infraestrutura de TIC continuará funcionando normalmente, mas poderemos estar expostos a riscos que não tomaremos conhecimento.

CRITÉRIOS DE ACEITAÇÃO

Item	Etapa/Entrega	Critério	Prazo/Periodicidade
1 e 2	Entrega das licenças	Licenças entregues e registradas na solução	30 dias
3	Instalação	Solução implantada com um pelo menos 128 ativos sendo monitorados	30 dias
4	Treinamento	Treinamento realizado	30 dias
5	Serviço Especializado	Adesão por demanda	7 dias

MECANISMOS FORMAIS DE COMUNICAÇÃO

Função	Forma	Periodicidade	Emissor	Destinatário
(x) Abertura de chamado	Telefone, e-mail, sistemas web	Por demanda	TRE-RS	Fabricante
(x) Encaminhamento de Ordem de Serviço	Telefone, e-mail, sistemas web	Por demanda	TRE-RS	Fornecedor
( ) Encaminhamento de NFs				

( ) Outra:				

CRITÉRIOS DE SELEÇÃO DO FORNECEDOR	
REQUISITOS DO FORNECEDOR	
Requisito:	**Justificativa:**
(x) Atestado de capacidade técnica fornecido por pessoa jurídica de direito público ou privado, no qual esteja expressa a aptidão do interessadono fornecimento regular, 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.	- evitar a participação de empresas que não são do ramo ou que tenham interesse apenas em adquirir e repassar as licenças. Considerando que parte da contratação é composta por serviços (instalação, treinamento, serviço especializado), faz-se necessário este requisito.
(x) Outros: 1) 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. 2) a fabricante deverá possuir os seguintes selos de segurança da informação EU-U.S. Privacy Shield Framework e Swiss-U.S. Privacy Shield Framework.	1) Para garantir que a empresa contratada é credenciada junto ao fabricante. 2) Como são soluções fornecidas globalmente e como nossa legislação sobre Proteção de Dados é muito recente, essas soluções não possuem certificação para LGPD. Por outro lado, devemos ter preocupação a respeito das informações sobre vulnerabilidades que estarão de posse do fornecedor. Subsidiariamente, precisamos solicitar selos que garantam bons níveis de privacidade desses dados. Durante a pesquisa de mercado, verificou-se que os fornecedores são capazes de atender a esses selos, portanto podemos solicitá-los sem prejudicar a concorrência.

REQUISITOS DA EQUIPE TÉCNICA			
Papel:	**Qtd**	**Requisito:**	**Justificativa:**
Profissional Especializado	1	**( )** Formação em:	
		(x) Certificação em: do fabricante da solução	Certificação oficial do fabricante da solução
		( ) Experiência, comprovada através de currículo, em:	

Equipe de Planejamento da Contratação
Márcio Barbosa de Carvalho Integrante Demandante
Rodrigo Bueno Cantini

Integrante Técnico

José Atílio Benites Lopes

Integrante Administrativo

Documento assinado eletronicamente por **Rodrigo Bueno Cantini**, **Técnico Judiciário**, em 08/10/2020, às 13:02, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Marcio Barbosa de Carvalho**, **Técnico Judiciário**, em 13/10/2020, às 18:57, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-rs.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0447291** e o código CRC **E4244F15**.

JUSTIÇA ELEITORAL
TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO SUL

Administração - Aquisição - Bens de Consumo - 0009384-54.2020.6.21.8000
Termo de Referência - TR - doc. SEI n. 0447504.

1 OBJETO

1.1 Descrição

Contratação de Solução para Avaliação de Vulnerabilidades em Ativos de Informação e para Avaliação Dinâmica de Aplicações WEB hospedada em nuvem pública (no modelo Software as a Service - SaaS) compreendendo aquisição de licenças de software e suporte técnico para um período de 60 meses, bem como serviço de instalação, treinamento e de serviço especializado.

2 FUNDAMENTAÇÃO DA CONTRATAÇÃO

2.1 Motivação

A gestão de vulnerabilidades é um processo complementar ao de gestão de eventos de segurança da informação realizado pelo SIEM, que foi implantado no início de 2020 no TRE-RS. Esse processo preocupa-se com a descoberta e remediação de vulnerabilidades que podem estar presentes nos sistemas de informação. Uma vulnerabilidade pode surgir pela utilização de uma versão comprometida de um software ou por uma configuração inadequada desse software. Essa vulnerabilidade pode ser explorada por um atacante para prejudicar a disponibilidade, integridade e confidencialidade dos ativos de informação. Devido à complexidade e quantidade de ativos de informação utilizados no nosso ambiente de TIC, o processo de gestão de vulnerabilidades necessita ser suportado por uma solução de gestão de vulnerabilidades. Essa solução deverá monitorar os ativos de informação da infraestrutura de TIC do TRE e apontar suas vulnerabilidades, suportando o processo de gestão de vulnerabilidades e gerando incidentes de segurança no IBM Qradar.

Além disso, muitas das aplicações utilizadas no TRE-RS foram desenvolvidas internamente pela STI, pelo TSE ou por terceiros. Por serem de finalidade específica e não serem públicas, essas aplicações não são avaliadas pelas organizações que mantém bases de dados sobre vulnerabilidades. Por outro lado, essas aplicações são tão (ou mais) sensíveis que softwares de uso geral e podem conter vulnerabilidades em sua programação. Para avaliar a programação dessas aplicações, é necessária a utilização de uma solução de avaliação dinâmica, que consiste em expor a aplicação a tentativas de exploração (por exemplo, SQL injection, cross-site scripting (XSS)) que seriam utilizadas por um atacante para detectar se são suscetíveis a essas técnicas de exploração.

2.2 Objetivos a serem alcançados por meio da contratação

• Identificação das vulnerabilidades das soluções de TIC utilizadas pelo TRE-RS.
• Redução do nível de risco através da redução da probabilidade de ameaças explorarem as vulnerabilidades de nossos ativos.
• Aderência do TRE-RS às boas práticas de segurança aconselhadas pelo Gartner e definidas na CIS Controls (Center of Internet Security Controls).

2.3 Benefícios diretos e indiretos alcançados por meio da contratação

A solução em nuvem no modelo SaaS oferece a vantagem de não requerer a disponibilização de recursos computacionais da infraestrutura de TIC do TRE-RS. Além disso, parte da gerência da solução (atualização, instalação de patches) é realizada pelo fornecedor da solução.

2.4 Alinhamento entre a contratação e o planejamento existente

A presente contratação faz parte dos objetivos, metas e ações do planejamento do TRE e STI:

2.4.1 Planejamento estratégico institucional

2.4.1.1 Está alinhado ao objetivo Aperfeiçoar a infraestrutura de TI.

2.4.2 Planejamento estratégico de TI (PETI)

2.4.2.1 Está alinhada ao Objetivo 6 – Aprimorar a gestão de riscos de TIC

2.4.3 Plano Diretor de TI (PDTI)

A ação refente a esta contratação consta no PDTIC sob o código 247.01

2.4.4 Plano de Contratações

2.4.4.1 A contratação consta do Plano de Contratações de 2020, identificada sob o ID 11258.

2.5 Referência aos estudos preliminares

Para a presente contratação foram elaborados os estudos preliminares, com as etapas de Análise da Viabilidade da Contratação, Sustentação do Contrato, Estratégia para a Contratação e Análise de Riscos, relatados nos documentos 0444604, 0445040, 0447291 e 0447443 do processo SEI 0009384-54.2020.6.21.8000. Os estudos foram elaborados de acordo com a IN 39/2014, da Presidência do TRE-RS.

2.6 Relação entre a demanda prevista e quantidade de bens a serem contratados

Ao avaliar o tamanho atual do parque computacional do TRE-RS, foi realizada uma estimativa de que são necessárias 500 licenças para avaliação de vulnerabilidades e serão registradas mais 128 licenças para eventual crescimento. Quanto às aplicações, estima-se que 10 aplicações possam ser objeto de análise simultaneamente e serão registradas mais 5 licenças para eventual crescimento.

2.7 Análise do mercado de Tecnologia da Informação e justificativa da escolha da solução

Foram realizados estudos em pesquisas e materiais do Gartner para um entendimento global de soluções para avaliação de vulnerabilidades. A partir desse estudo, foi elaborada uma lista de requisitos tecnológicos, que foram avaliados também por um analista do Gartner. Dois grandes grupos de soluções atenderiam nossos requisitos tecnológicos: software ofertado por subscrição hospedado na infraestrutura computacional do cliente (on premise) ou hospedado em nuvem pública no modelo SaaS. Nos estudos, foi identificada vantagem para soluções ofertadas no modelo SaaS por receberem mais atenção dos fornecedores devido a uma tendência de mercado de que tais soluções sejam mais ofertadas em nuvem do que on premise, portanto para manter competitividade essas soluções recebem mais incremento de funcionalidades do que aquelas ofertadas on premise. Embora a solução no modelo SaaS tenha um custo maior do que a solução no modelo on premise, há de se considerar que o TRE-RS não precisaria arcar com o custo operacional e da infraestrutura computacional no modelo SaaS. Portanto, a diferença de custo da solução em nuvem está adequado e competitivo em relação ao modelo on premise.

2.8 Natureza do objeto

O objeto pretendido é de natureza comum no âmbito do mercado de tecnologia da informação.

2.9 Parcelamento do objeto

O objeto deverá ser adjudicado por lotes de itens.

2.10 Seleção do Fornecedor

As vulnerabilidades identificadas pelos itens 1 e 2 deverão ser priorizadas seguindo um mesmo processo de tratamento que leva em consideração as capacidades de remediação das equipes de TIC. Portanto, como serão tratadas pelo mesmo processo, é necessário que estejam em uma mesma solução. Além disso, ao se identificar um conjunto de vulnerabilidades em um ativo (identificadas tanto pelo item 1 ou pelo item 2) pode-se chegar a conclusão que uma remediação mais abrangente seja mais adequada. A visão dessas vulnerabilidades em uma solução única facilita o planejamento de remediações atinentes a um mesmo ativo.

Os itens 3, 4 e 5 são referentes ao que for entregue nos itens 1 e 2, por esse motivo fazem parte do mesmo lote.

2.11 Impacto ambiental

Não há impacto ambiental.

3 DESCRIÇÃO DA SOLUÇÃO

3.1 Detalhamento do objeto

Item	Descrição do equipamento	Siasg	Unidade	Quantidade
1	Licença da solução de avaliação de vulnerabilidades por endereço IP ou ativo por 5 anos	27464	Un.	**1x500 + 1x128**
2	Licença da solução de avaliação dinâmica de aplicações por FQDN (*Full Qualified Domain Name*) por 5 anos	27464	Un.	**1x10 + 1x5**
3	Serviço de instalação e configuração	26972	Un.	**1**
4	Repasse tecnológico de 20 horas para até 10 servidores	3840	Un.	**1**
5	Bloco de 4 horas de serviço especializado	26972	Un.	**10**

4 ESPECIFICAÇÃO TÉCNICA

4.1 Requisitos técnicos gerais da solução. Características mínimas:

4.1.1 A solução deve estar licenciada 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 mínimo 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:

4.1.24.1 Execução de verificação completa do sistema (rede), adequada para qualquer host.

4.1.24.2 Verificação sem recomendações da rede, para que se possa personalizar totalmente as configurações da verificação.

4.1.24.3 Autenticação de hosts e enumeração de atualizações ausentes.

4.1.24.4 Execução de varredura simples para descobrir hosts ativos e portas abertas.

4.1.24.5 Utilização de um scanner para verificar aplicativos da web.

4.1.24.6 Avaliação de dispositivos móveis.

4.1.24.7 Auditoria de configuração de serviços em nuvem de terceiros.

4.1.24.8 Auditoria de configuração dos gerenciadores de dispositivos móveis.

4.1.24.9 Auditoria de configuração dos dispositivos de rede.

4.1.24.10 Auditoria de configurações do sistema em relação a uma linha de base conhecida.

4.1.24.11 Detecção de desvio de segurança Intel AMT.

4.1.24.12 Verificação de malware nos sistemas Windows e Unix.

4.1.25 Deve ser possível determinar quais portas de serviços (UDP/TCP) estão abertas em determinado ativo em tempo real.

4.1.26 A solução deve ser capaz de realizar em tempo real a descoberta de novos ativos para no mínimo:

4.1.26.1 Bancos de dados.

4.1.26.2 Hypervisors (no mímino VMWare ESX/ESXi).

4.1.26.3 Dispositivos móveis.

4.1.26.4 Dispositivos de rede.

4.1.26.5 Endpoints.

4.1.26.6 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:

4.1.32.1 Todos os dados armazenados nos servidores da solução devem ser criptografados e possuir logs de acesso.

4.1.32.2 Os dados em trânsito devem usar ao menos o algoritmo TLS 1.2 de chave 2048 bits.

4.1.32.3 Os dados em trânsito devem ser criptografados ao menos com o algoritmo AES-128 bits.

4.1.32.4 Os algoritmos de hash devem usar ao menos o algoritmo SHA-256.

4.1.32.5 Será aceito como comprovação critérios de criptografia publicados no site do fabricante ou declaração do próprio fabricante.

4.1.32.6 Os dados armazenados devem ser criptografados ao menos com o algoritmo AES-256 bits.

4.1.32.7 Somente servidores da Contratante ou pessoa por ela autorizada poderão ter acesso aos dados da solução.

4.1.32.8 A solução deve permitir a criação de, no mínimo, 20 contas para gerência e acesso aos relatórios, sem custo adicional.

4.1.32.9 A empresa contratada não deverá ter acesso à rede interna da contratante e todo tráfego 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 críticas.

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.

4.1.40 A solução deve ser baseada em nuvem pública, com scanners próprios localizados em nuvem pública e scanners instalados na infraestrutura do cliente (on premises).

4.1.41 A solução deve possuir índice de disponibilidade mensal e anual maior ou igual a 99%.

4.1.42 As soluções propostas nos itens 1 e 2 devem ser de mesmo fabricante, sem adaptações ou alterações não efetuadas pelo fabricante, disponível para gerenciamento em console central web unificado, sendo toda infraestrutura de aplicações, bancos de dados de vulnerabilidades, dashboards, agentes e plugins também mantidas pelo mesmo fabricante, oferecida como serviço padrão.

4.1.43 Configuração de segurança e acesso à gerência da solução:

4.1.43.1 A solução deve suportar autenticação de dois fatores para os usuários.

4.1.43.2 A solução deve possuir proteção contra ataques de força bruta bloqueando as contas após um número determinado de tentativas de login malsucedidas.

4.1.43.3 Os dados da CONTRATANTE devem ser marcados com um identificador que corresponde a assinatura específica da CONTRATANTE de forma a garantir que o acesso aos dados da CONTRATANTE seja limitado a apenas a CONTRATANTE.

4.1.44 A solução deve possuir conectores para, no mínimo, as seguintes plataformas:

4.1.44.1 Amazon Web Service (AWS).

4.1.44.2 Microsoft Azure.

4.1.44.3 Google Clound Platform.

4.1.45 A fabricante deve possuir no mínimo as seguintes certificações de privacidade e segurança:

4.1.45.1 EU-U.S. Privacy Shield Framework.

4.1.45.2 Swiss-U.S. Privacy Shield Framework.

4.2 Características técnicas da Solução de Avaliação de Vulnerabilidades (item 1). Características 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 técnicas da Solução de Avaliação Dinâmica de Aplicações WEB (item 2). Características mínimas:

4.3.1 A solução de análise deve realizar varreduras de vulnerabilidades em aplicações Web, cobrindo no mínimo, mas não limitando-se à 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:

4.3.5.1 Cookies, Headers, Formulários e Links.

4.3.5.2 Nomes e valores de parâmetros da aplicação.

4.3.5.3 Elementos JSON e XML.

4.3.5.4 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:

4.3.13.1 Número máximo de URLs para crawling e navegação.

4.3.13.2 Número máximo de diretórios para varreduras.

4.3.13.3 Tamanho máximo de respostas.

4.3.13.4 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 e-mail.

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:

4.3.17.1 Autenticação Básica (Digest).

4.3.17.2 NTLM.

4.3.17.3 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:

4.3.23.1 WordPress.

4.3.23.2 IIS 6.x e IIS 10.x.

4.3.23.3 ASP 6.

4.3.23.4 .NET 2.

4.3.23.5 Apache HTTPD 2.2.x e 2.4.x.

4.3.23.6 Tomcat 6.x, 7.x, 8.x e superiores.

4.3.23.7 Jetty 8 e superiores.

4.3.23.8 Nginx.

4.3.23.9 PHP 5.3.x, 5.4.x, 5.6.x, 7.0.x e 7.1.x e superiores.

4.3.23.10 Java 1.5, 1.6, 1.7 e 1.8 e superiores.

4.3.23.11 Jboss 4.x e 7.x e superiores.

4.3.23.12 WildFly 8 e 10 e superiores.

4.3.23.13 Plone 2.5.x e 4.3.x e superiores.

4.3.23.14 Zope.

4.3.23.15 Python 2.4.4 e superiores.

4.3.23.16 J2EE.

4.3.23.17 Ansible.

4.3.23.18 Joomla.

4.3.23.19 Moodle.

4.3.23.20 Docker Container.

4.3.23.21 Elk.

4.3.23.22 GIT.

4.3.23.23 Grafana.

4.3.23.24 Redmine.

4.4 Características técnicas da Instalação e Configuração (item 3). Características 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 pela 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 serviço de Instalação e Configuração (item 3).

4.5 Características técnicas do Repasse Tecnológico. Características 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:

4.5.2.1 Procedimentos de instalação física e lógica.

4.5.2.2 Todos os procedimentos necessários à configuração técnica.

4.5.2.3 Todos os procedimentos necessários à completa operação do produto.

4.5.2.4 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 (item 4).

4.6 Características técnicas do Bloco de 04 Horas de Serviço Especializado (item 5). Características 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:

4.6.1.1 Acompanhar, quando solicitado por um usuário, todas as operações realizadas no sistema durante determinado período de tempo.

4.6.1.2 Esclarecer dúvidas de usuários em relação à operação do sistema.

4.6.1.3 Prestar serviços de suporte técnico para a solução de problemas que impeçam o perfeito funcionamento do sistema.

4.6.1.4 Reportar à Coordenação de informática do órgão quaisquer outros problemas verificados durante o atendimento, relativos ou não à solução fornecida.

4.6.1.5 Fornecer informações aos usuários sobre a situação e o andamento de serviços de manutenção solicitados.

4.6.1.6 Diagnosticar a performance do software em seus aspectos operacionais.

4.6.1.7 Identificar problemas inerentes ao software e ao ambiente onde este se encontra instalado.

4.6.1.8 Discutir implementações de melhorias, visando possíveis adequações.

4.6.1.9 Na prestação dos serviços de operação assistida, a Contratada deverá utilizar profissionais com qualificação e treinamento adequados para o desenvolvimento das tarefas relacionadas anteriormente.

4.6.1.10 Apoio no desenvolvimento de dashboards e solução de problemas internos, relativos às licenças adquiridas.

4.6.1.11 Integração da solução com ferramentas de ITSM.

4.6.1.12 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.

4.6.3 O licitante poderá apresentar R$ 0,00 (zero reais) como o preço dos itens relacionados ao Bloco de 04 Horas de Serviço Especializado (item 5) caso os serviços elencados estejam incluídos no preço da solução ofertada da ferramenta de gestão de vulnerabilidades.

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 (item 5).

5 MODELO DE EXECUÇÃO DO OBJETO

5.1 Prazos e condições

5.1.1 As licenças de software necessárias para o atendimento do Termo de Referência deverão ser disponibilizadas num prazo de cinco (cinco) dias úteis, a contar do aceite da nota de empenho, por meio de e-mail para segti@tre-rs.jus.br.

5.1.2 Constatada a ocorrência de divergência na especificação do produto entregue, fica a CONTRATADA obrigada a providenciar a substituição em até 05 (cinco) dias corridos, contados a partir do recebimento da notificação da ocorrência por parte da CONTRATANTE.

5.1.3 Agendamento dos itens 3 e 4 enviar e-mail para segti@tre-rs.jus.br.

5.1.4 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.

5.1.5 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.

5.1.6 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 registrado no item 5.

5.1.7 A Contratada deverá:

5.1.7.1 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.

5.1.7.2 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:

5.1.7.2.1 Apresentação de declaração do fabricante da solução ofertada no item 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;

5.1.7.2.2 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 a este órgão no âmbito da presente contratação.

5.1.7.2.3 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.

5.1.7.2.4 O técnico deverá estar devidamente contratado pela empresa fornecedora da solução.

5.2 Forma de prestação da garantia e do suporte técnico

5.2.1 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.

5.2.2 O suporte pelo fabricante será obrigatório.

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

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

5.2.5 O tempo da garantia e suporte técnico dos itens 1 e 2 é de 60 meses.

5.2.6 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.

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

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

5.2.8.1 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).

5.2.8.2 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).

5.2.8.3 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).

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

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

5.2.11 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.

5.2.12 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.

5.2.13 Os chamados abertos por e-mail deverão ter sua abertura automática no portal web.

5.2.14 Todo o chamado aberto deverá ter sua resolução técnica registrada no sistema web de help-desk.

5.2.15 A contratante poderá solicitar o escalonamento de incidentes ao fabricante quando se tratarem de correções especiais, defeitos nos programas ou defeito em hardware.

5.2.16 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.

5.2.17 A garantia iniciará sua contagem a partir da data de emissão da NF dos softwares, serviços ou licenças.

5.2.18 Havendo discrepâncias entre o que está especificado no item específico e o que consta nestas condições gerais, prevalecerá o que está no item específico.

5.3 Obrigações do Contratante

5.3.1 Receber provisoriamente o material, disponibilizando local, data e horário.

5.3.2 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 definitivo.

5.3.3 Acompanhar e fiscalizar o cumprimento das obrigações da Contratada, através do gestor e dos fiscais especialmente designados.

5.3.4 Efetuar o pagamento na forma e no prazo previsto neste instrumento e no contrato.

5.4 Obrigações da Contratada

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 de 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.

5.4.3 Fornecer todas as licenças de software necessárias para utilização completa da solução, pelos períodos adquiridos.

5.4.4 Registrar, junto aos fabricantes e em nome da contratante, todas as assinaturas de licenças de software ofertadas.

5.4.5 Cumprir fielmente as obrigações assumidas, conforme as especificações constantes neste Termo de Referência, utilizando-se de todos os recursos materiais e humanos necessários para entregar os produtos/prestar os serviços, nos prazos indicados.

5.4.6 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.

5.4.7 Prestar todos os esclarecimentos que forem solicitados pelo TRE-RS, credenciando junto ao órgão, um representante para prestar os devidos esclarecimentos e atender as reclamações que porventura surgirem durante a execução do objeto.

5.4.8 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.

5.4.9 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.

5.4.10 Executar os serviços nos prazos estabelecidos neste instrumento, nos locais indicados pela Administração, em estrita observância das especificações do Edital e da proposta.

5.4.11 Atender prontamente aos chamados da Administração, relacionados ao objeto da licitação.

5.4.12 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.

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

5.4.14 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.

5.4.15 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.

5.4.16 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.

6 MODELO PARA GESTÃO DA CONTRATAÇÃO

6.1 Papéis a serem desempenhados

6.1.1 Fiscal técnico

6.1.1.1 Verificar a conformidade das especificações das licenças entregues com o constante neste termo de referência.

6.1.1.2 Avaliar a conformidade dos serviços prestados com as especificações constantes neste termo de referência.

6.1.2 Gestor:

6.1.2.1 Baseado nas informações prestadas pelo Fiscal Técnico proceder o aceite definitivo das licenças e serviços e encaminhar as notas fiscais para pagamento.

6.2 Mecanismos formais de comunicação

A comunicação entre as partes se dará por escrito, através de e-mail endereçados aos gestores do contrato designados pelas partes, exceto a abertura de chamados de garantia, que poderá ser realizada também por telefone ou aplicativo web.

6.3 Metodologia de avaliação da qualidade do objeto

O objeto será avaliado apenas quanto ao atendimento dos requisitos exigidos na especificação técnica.

6.4 Forma de recebimento

6.4.1 Para os itens 1 e 2: o fornecimento das licenças de software deverá ocorrer em até 05 (cinco) dias úteis após o aceite da nota de empenho.

6.4.2 Para o item 3: 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.

6.4.3 Para o item 4: 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.

6.4.4 O item 5: 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.

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

6.4.6 Os serviços devem ser agendados com antecedência mínima de 5 dias sob o risco de não serem autorizados.

6.4.7 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.

6.4.8 Para itens de software, devem ser apresentadas chaves únicas tipo serial ou qualquer outra forma de validação da ferramenta, comprovando perante o fabricante que trata-se de uma ferramenta devidamente licenciada.

6.4.9 O Termo de Recebimento Provisório será emitido por servidor ou comissão do TRE-RS, devidamente constituída para este fim, em até 5 dias úteis após a entrega dos itens.

6.4.10 O Termo de Recebimento Definitivo será emitido por servidor ou comissão do TRE-RS devidamente constituída para este fim em até 10 dias úteis após a entrega.

6.5 Condições para pagamento

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

6.6 Penalidades

6.6.1 O CONTRATANTE poderá aplicar à CONTRATADA as penalidades previstas no artigo 28 do Decreto nº 5.450/2005. A Administração poderá, ainda, a seu critério, utilizar-se subsidiariamente das sanções previstas na Lei nº 8.666/93, no que couber.

6.6.2 A recusa injustificada do adjudicatário em retirar a Nota de Empenho ou 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.

6.6.3 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 6.6.4 e do impedimento para licitar e contratar com a União, nos termos do art. 28 da do Decreto nº 5.450/2005.

6.6.4 Com fundamento no art. 28 da do Decreto nº 5.450/2005, 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:

6.6.4.1 Apresentar documentação falsa.

6.6.4.2 Ensejar o retardamento da execução do seu objeto.

6.6.4.3 Falhar ou fraudar na execução do contrato.

6.6.4.4 Comportar-se de modo inidôneo.

6.6.4.5 Fizer declaração falsa.

6.6.4.6 Cometer fraude fiscal.

6.6.4.7 Não mantiver a proposta.

6.6.4.8 Deixar de entregar documentação exigida no edital e no termo de referência.

6.6.5 Para os fins do item 6.6.4, reputar-se-ão inidôneos atos como os descritos nos arts. 90, 92, 93, 94, 95 e 97 da Lei nº 8.666/93.

6.6.6 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:

6.6.6.1 Multa moratória de:

6.6.6.1.1 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.

6.6.6.1.2 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 6.6.4, 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.

6.6.7 As multas moratória e compensatória poderão ser cumuladas com as sanções previstas no item 6.6.1.

6.6.8 Apenas a aplicação das penalidades de advertência e multa moratória, não necessitam ser publicadas no DOU, devendo a intimação da apenada dar-se por meio de notificação.

6.6.9 As sanções estabelecidas nesta cláusula são da competência exclusiva da autoridade designada nos normativos internos deste Tribunal, facultada a defesa do interessado no respectivo processo, no prazo legal.

6.6.10 A autoridade competente, na aplicação das penalidades previstas nesta cláusula, deverá levar em consideração a gravidade da conduta da Contratada, o caráter educativo da pena, bem como o dano causado ao Contratante, observados os princípios da proporcionalidade, da razoabilidade, da prevalência e indisponibilidade do interesse público, em decorrência de circunstâncias fundamentadas em fatos reais e comprovados.

6.6.11 O valor da multa moratória ou compensatória, nos termos do artigo 86, § 3º da LLC, poderá ser descontado da garantia contratual, dos créditos da Contratada ou cobrado judicialmente, nesta ordem.

6.6.12 O recolhimento do valor da multa, moratória ou compensatória, deverá ser feito no prazo de 5 (cinco) dias úteis contados da data da intimação da aplicação da sanção, sob pena de seu desconto ser efetuado conforme item anterior, acrescida de juros moratórios de 1% (um por cento) ao mês.

6.6.13 As penalidades estabelecidas nesta cláusula deverão ser registradas no SICAF.

6.6.14 As penalidades descritas nesta cláusula não excluem a possibilidade de o CONTRATANTE cobrar da CONTRATADA indenização por eventuais perdas e danos.

6.7 Transferência de conhecimento e dos direitos de propriedade intelectual

A transferência de conhecimento se dará através de acompanhamento dos serviços de instalação e configuração.

Equipe de Planejamento da Contratação
Márcio Barbosa de Carvalho Integrante demandante
Rodrigo Bueno Cantini Integrante técnico
José Atilio Benites Lopes Integrante administrativo

Documento assinado eletronicamente por **Rodrigo Bueno Cantini**, **Técnico Judiciário**, em 08/10/2020, às 13:04, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Marcio Barbosa de Carvalho**, **Técnico Judiciário**, em 13/10/2020, às 18:57, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-rs.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0447504** e o código CRC **66081F12**.