TRIBUNAL REGIONAL DO TRABALHO DA 12ª REGIÃO

ESTUDOS PRELIMINARES DE CONTRATAÇÃO DE SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

PROAD: 5130/2022

1. Capítulo I - ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO

1.1. Objeto

Aquisição de solução que auxilie na prevenção e limitação da extensão de ataques cibernéticos, através do gerenciamento de vulnerabilidades, baseada em risco, dos ativos de Tecnologia da Informação, com análise contínua e adaptável de riscos e confiança, a fim de manter a confidencialidade, a disponibilidade e a integridade das informações.

1.2. Justificativa

Somente no primeiro trimestre de 2021, o Brasil teve 3,2 bilhões de tentativas de ataques cibernéticos, sendo o principal alvo na América Latina[1]. Com o aumento destas tentativas de ataques, faz-se mister fortalecer a segurança da informação deste Egrégio Tribunal, através da adoção de medidas necessárias para mitigar as fragilidades do ambiente computacional.

Nos últimos três anos, foram diversos os ataques cibernéticos realizados no Brasil contra órgãos do Governo, podemos citar: Ministério da Saúde, Controladoria Geral da União, Polícia Rodoviária Federal, Superior Tribunal de Justiça, Tribunal de Justiça do Rio Grande do Sul, Tribunal Regional do Trabalho da 4ª Região, da 17ª Região, Tribunal Regional Federal da 3ª Região, Tribunal de Contas do Estado de Santa Catarina, entre diversos outros.

---

[1] Disponível em: https://www.fortinet.com/br/corporate/about-us/newsroom/press-releases/2021/brasil-comeca-ano-com-mais-3-2-billhoes-tentativas-de-ciberataques com acesso em 1-7-2022.

Ademais, com a Lei Geral de Proteção de Dados brasileira, todos os órgãos públicos deverão investir em segurança e implementar processos e tecnologias efetivos para prevenir, detectar e remediar violações de dados pessoais.

A análise de vulnerabilidade é fundamental neste cenário, pois promove a melhoria contínua da infraestrutura num processo de definição, classificação e hierarquização dos recursos; identificação das ameaças existentes para cada um deles; estabelecendo estratégias para cada ameaça identificada e monitorando constantemente.

Ela é instrumento para administrar e melhorar a confidencialidade, disponibilidade e integridade das informações dos magistrados, servidores e principalmente dos jurisdicionados do Tribunal.

Desta forma, a Análise de Vulnerabilidades é de suma relevância para avaliação adaptativa contínua de riscos e confiança dos ativos de tecnologia da informação, aumento da conformidade regulatória e proteção das informações da Justiça do Trabalho. Como especificado na regulamentação interna do Judiciário, especificamente do Guia da Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário ENTIC-JUD 2021-2026[2], que, em seu Capítulo 5, prevê a necessidade de“Aprimorar Segurança da Informação e a Gestão de Dados”.

Dentre os benefícios, destacam-se a redução de riscos e vulnerabilidades dos sistemas deste Regional, identificando-os de forma periódica e orientada à riscos; a redução do risco de vazamento de informações da justiça do trabalho, dos magistrados, servidores e jurisdicionados; garantia da continuidade do negócio do TRT da 12ª Região; e da preservação da imagem institucional.

Além disso, uma solução em gerenciamento permite a varredura de vulnerabilidades dos ativos de tecnologia da informação (equipamentos como Servidores de dados, estações de trabalho, telefones ip, switches, câmeras ip), de forma periódica e orientada a riscos, provendo relatórios detalhados e ações que tornam os ativos mais seguros e eficientes. Esta solução também oferece funcionalidades como gestão de baselines, compliance e atribuição de scores aos ativos escaneados.

---

[2] O Guia da Estratégia Nacional de TIC do Poder Judiciário ENTIC-JUD 2021-2026 está disponível em https://atos.cnj.jus.br/files/compilado184145202110266178 4be9efedd.pdf, acessado em 28 de junho de 2022.

Considerando todos os ataques que os sistemas de informática têm recebido, principalmente no setor público, e considerando os dados sensíveis que esta instituição guarda, e a necessidade de manter os sistemas confiáveis, pois apesar de possuirmos sistemas de proteção tais como Firewall e antivírus entre outros, eles não protegem contra falhas dos softwares dos sistemas nacionais ou não, desenvolvidos dentro dos Tribunais, e falhas decorrentes de configurações realizadas para manter os serviços hoje disponíveis como PJE, Folha de Pagamento, SIGEP, SIGEC etc …

1.3. Quantidade

Item	Descrição	QTDE	UNIDADE	Despesa
1	Solução de Gerenciamento de vulnerabilidades para **FQDNs Externos**, dos ativos de Tecnologia da Informação, baseada e com análise contínua e adaptável de riscos e confiança, com o serviço de implantação e também o de garantia dos equipamentos e/ou softwares pelo período de 60 meses.	50	Licença	GND4
2	Solução de Gerenciamento de vulnerabilidades para **FQDNs Internos**, dos ativos de Tecnologia da Informação, baseada e com análise contínua e adaptável de riscos e confiança, com o serviço de implantação e também o de garantia dos equipamentos e/ou softwares pelo período de 60 meses.	60	Licença	GND4
3	Solução de Gerenciamento de vulnerabilidades para **Imagens de aplicações em Container**, baseada e com análise contínua e adaptável de riscos e confiança, com o serviço de implantação e também o de garantia dos equipamentos e/ou softwares pelo período de 60 meses.	150	Licença	GND4
4	Solução de Gerenciamento de vulnerabilidades para **Endpoints**, baseada e com análise contínua e adaptável de riscos e confiança, com o serviço de implantação e também o de garantia dos equipamentos e/ou softwares pelo período de 60 meses.	1500	Licença	GND4
5	Suporte técnico especializado.	60	Meses	GND3

6	Treinamento técnico da Solução de Gerenciamento de vulnerabilidades.	6	Pessoas	GND3

ITEM 1: Solução de Gerenciamento de vulnerabilidades para **FQDNs[3] Externos**:

Foi realizado levantamento, pela equipe de infraestrutura, que apontou uma demanda ao longo do contrato de aproximadamente **50 FQDNs externos**.

ITEM 2: Solução de Gerenciamento de vulnerabilidades para **FQDNs Internos**:

Foi realizado levantamento, pela equipe de infraestrutura, que apontou uma demanda ao longo do contrato de aproximadamente **60 FQDNs internos.**

ITEM 3: Solução de Gerenciamento de vulnerabilidades para **Imagens de aplicações em Container**:

Questionada sobre o número imagens de container, existentes em produção, a equipe de infraestrutura respondeu que, a demanda ao longo do contrato é de aproximadamente de **150 imagens únicas**.

ITEM 4: Solução de Gerenciamento de vulnerabilidades para **Endpoints**:

Foi utilizado o último levantamento realizado pela equipe de infraestrutura, a qual apontou **3000 endpoints**. Para sessenta meses de contrato, e por ser um parque de estações mais homogêneo, não há a necessidade de licenciar todos os endpoints, desta forma, definimos o valor de **1.500 Endpoints**.

ITEM 5: Suporte técnico especializado:

[3] FQDNs: Nome de Domínio Completamente Qualificado é um nome de domínio que especifica sua localização exata na árvore hierárquica do Domain Name System (DNS). Ele pode ser de acesso externo, como: www.trt12.jus.br, correio.trt12.jus.br; ou de acesso interno: abba.trt12.jus.br, intranet.trt12.jus.br

Foi utilizado o prazo compatível com o período das soluções dos Itens 1 ao 4, ou seja, 60 meses.

ITEM 6: Treinamento

Foi considerada a quantidade de servidores que darão suporte ao produto, sendo, 4 servidores do Seinfra, 1 do Sesup e 1 do Seginfo.

1.4 Definição e Especificação dos Requisitos.

1.4.1. O licenciamento da plataforma deverá ser por ativo, sendo este um dos abaixo:

1.4.1.1. Ativos em rede;

1.4.1.2. Servidores e Estações de trabalho ou Notebooks;

1.4.1.3. Servidores em Cloud;

1.4.1.4. Contêineres;

1.4.1.5. Aplicações Web e API;

1.4.2. O licenciamento poderá ser flexível, ou seja, não limitado por módulo.

1.4.3. O gerenciamento da plataforma deverá ser centralizado e único para todos os módulos descritos neste documento;

1.4.4. A solução deve fornecer alta disponibilidade, com cluster ativo – ativo, no site principal e site backup, com redundância da base de dados entre os sites.

1.4.5. Plataforma de Gestão de Vulnerabilidade em Ativos de Rede e Nuvem.

1.4.6. Controle de Usuários, a ferramenta deve gerenciar e controlar os os acessos e usuários

1.4.7. A ferramenta deve possuir Relatórios e Dashboards, a fim de auxiliar o uso e melhorar a experiência do usuário

1.4.8. A ferramenta deve ter Conformidade e Compliance

1.4.9. Possuir Plataforma de Gestão de Vulnerabilidade em Aplicações Web

1.4.10. Possuir Plataforma de Gestão de Vulnerabilidade em Contêineres

1.4.11. Ser capaz de prestar Suporte Técnico Especializado.

1.4.12. Oferecer Treinamento técnico da Solução de Gerenciamento de vulnerabilidades.

1.5. Levantamento das alternativas existentes

Conforme estudo técnico, identificou-se quatro possíveis cenários para o Gerenciamento de Vulnerabilidades:

Cenário 1 - Desenvolver solução interna de Gerenciamento de Vulnerabilidades:

Tal alternativa necessita que a equipe de tecnologia da informação deste Tribunal desenvolva uma solução de hardware e software que realize os scans de vulnerabilidades, com relatórios, análise de riscos e compliance. Demandando bastante tempo, recursos humanos e investimento em qualificação da equipe em segurança da informação.

Cenário 2 - Utilização de Solução de software livre.

Não foi encontrada solução que atenda aos requisitos presentes neste documento, no Portal do Software Público Brasileiro (http://softwarepublico.gov.br).

As ferramentas gratuitas disponíveis para download e utilização são limitadas em funcionalidades, quantidade de scans realizados, relatórios gerados, tipos de ativos suportados e não possuem suporte técnico adequado, além disso, poucas englobam o processo de gerenciamento de vulnerabilidades, com análise de riscos e compliance, e os relatórios fornecidos pelas ferramentas não apresentam rastreabilidade das atividades já realizadas nos ativos e sistemas, tornando-as incompatíveis com as necessidades do Tribunal Regional do Trabalho da 12ª Região.

Cenário 3 - Solução consolidada no mercado que auxilie na prevenção e limitação da extensão de ataques cibernéticos, através do gerenciamento de vulnerabilidades 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. 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.

Cenário 4 - Solução consolidada no mercado que auxilie na prevenção e limitação da extensão de ataques cibernéticos, através do gerenciamento de vulnerabilidades, baseada em gerenciamento em rede local do tribunal (On premises).

As soluções baseadas em gerenciamento em rede local (On premises) costumam apresentar um valor de aquisição menor do que a Cenário 3 (On cloud), pois os dados são gerenciados na própria infraestrutura da contratante.

Apesar do Cenário 4 (On premise) trazer o trabalho de atualização para a equipe de infraestrutura de rede, ela possui um menor risco de vazamento de dados sensíveis (como relatório de vulnerabilidades dos ativos de TIC do tribunal) pois estes dados serão armazenados na rede local do Tribunal e não em nuvem pública. 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 do **Cenário 4,** é o fato de que, após o término do suporte, a SETIC continuará a ter acesso à ferramenta, embora sem o direito de recebimento de atualizações de versão e de novas vulnerabilidades.

	Característica	**Cenário 1**	**Cenário 2**	**Cenário 3**	**Cenário 4**
01	Fabricante/Fornecedor	TRT12	Diversos/ Software Livre	- Qualys -Tenable - Rapid7	- Tenable - Rapid7

02	Nome solução (modelo)	N/A	NMAP Open Vas	- VM e módulo WAS; - Tenable.io e módulo WAS; - IVM e módulo IAS	- Tenable.sc; - Nexpose e módulo AppSpider
03	Custo efetivo total (CET)	0	0	R$ 2500 por licença	R$ 2600 por licença
04	Forma de entrega	Construção Própria	Freeware	Licença	Licença
05	A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública Federal?	N/A	N/A	Sim	Sim
06	A Solução está disponível no Portal do Software Público Brasileiro?	N/A	N/A	N/A	N/A
07	A Solução é um software livre ou software público?	Não	Sim	Não	Não
08	A Solução é aderente às políticas, premissas e especificações técnicas definidas no MNI do Poder Judiciário? (quando houver intercâmbio de informações de processos judiciais)	N/A	N/A	N/A	N/A
09	A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	N/A	N/A	N/A	N/A
10	A Solução é aderente a orientações, premissas e especificações técnicas e funcionais do Moreq-Jus? (quando houver documentos digitais produzidos pelo Judiciário)	N/A	N/A	N/A	N/A

Contratações Públicas Similares

Foram encontradas as seguintes contratações, no âmbito da administração pública federal, similar, que atendem aos requisitos desta demanda:

a) MPDFT - Ministério Público do Distrito Federal e dos Territórios - Pregão Eletrônico n°062/2020 - Aquisição de Licenças Perpétuas de Solução de Gestão de Vulnerabilidades e Serviços Associados.
b) Tribunal Regional Eleitoral da Paraíba - TRE-PB - Pregão Eletrônico n° 037/2020 - Aquisição de solução unificada de Gestão de Vulnerabilidades em ativos de tecnologia da informação e aplicações web, compreendendo aquisição de serviços de software e suporte técnico.
c) Tribunal De Contas De Roraima - Pregão eletrônico 017/2021 - Aquisição de solução unificada de Gestão de Vulnerabilidades em ativos de tecnologia da informação e aplicações web, compreendendo aquisição de serviços de software e suporte técnico, para atender as necessidades do tribunal de contas do estado. por 36 (trinta e seis) meses
d) Ministério Público do Estado da Bahia - Pregão Eletrônico No 04/2022 - Prestação de serviços de gestão de vulnerabilidades e conformidade de configuração para Ativos e Aplicações Web, por meio de solução unificada, a englobar licenciamento em modelo de subscrição, instalação, implantação, suporte técnico e treinamento, conforme condições estabelecidas neste edital e seus anexos.
e) Base Administrativa Do Centro De Comunicações E Guerra Eletrônica Do Exército Pregão Eletrônico No 26/2021 - O objeto da presente licitação é a escolha da proposta mais vantajosa para a contratação de serviços de tecnologia da informação e comunicação de licença para utilização de software de análise de vulnerabilidade Tenable Network Security Nessus Professional por 36 (trinta e seis) meses

1.6. Justificativa da escolha da solução

Desta forma o cenário 1 fica prejudicada por não termos quadro de pessoal suficiente para este desenvolvimento, o cenário 2 como descrito acima não contempla todas as necessidades de verificação e proteção para garantir um mínimo de segurança além de demandarem uma maior sobrecarga de trabalho das equipes internas.

Os cenários 3 e 4 atendem aos requisitos da contratação, desta forma foram pesquisadas soluções no mercado, as principais destacadas abaixo.

Solução 1: F-Secure Elements Vulnerability Management.

Solução 2: Qualys Vulnerability Management.

Solução 3: Rapid7 InsightVM.

Solução 4: Tenable: Tenable Security Center.

Desta forma é possível contratar por licitação própria, ou utilizando a Ata de Registro de Preços. O Tribunal Regional do Trabalho da 8ª Região realizou Pregão Eletrônico para contratação de Solução que auxilie na prevenção e limitação de ataques cibernéticos, através de gerenciamento de vulnerabilidade,que culminou na Ata de Registro de Preços Nº 5/2022, gerenciada pelo TRT da 8ª Região, da qual este Regional é coparticipante.

Considerando a economia e as vantagens de uma solução para todos os Tribunais, que gera sinergia e favorece a troca de informações, nivelando o conhecimento. Com a utilização desta ata teremos todas as vantagens do Cenário 4, pois baseia-se no gerenciamento da rede local do tribunal, apresentando ainda menor preço e realizando gerenciamento de vulnerabilidades em ativos de tecnologia da informação além de testes em aplicações Web, sem o armazenamento de dados sensíveis em nuvem pública.

Estando os preços da Ata de Registro de Preços do TRT8 dentro dos valores praticados pelo mercado, esta equipe recomenda a sua utilização.

1.7. Especificação completa da solução escolhida

1.7.1. O licenciamento da plataforma deverá ser por ativo, sendo este um dos abaixo:

1.7.1.1. Ativos em rede;

1.7.1.2. Servidores e Estações de trabalho ou Notebooks;

1.7.1.3. Servidores em Cloud;

1.7.1.4. Contêineres;

1.7.1.5. Aplicações Web e API;

1.7.2. O licenciamento poderá ser flexível, ou seja, não limitado por módulo.

1.7.3. O gerenciamento da plataforma deverá ser centralizado e único para todos os módulos descritos neste documento;

1.7.4. A solução deve fornecer alta disponibilidade, com cluster ativo – ativo, no site principal e site backup, com redundância da base de dados entre os sites.

1.7.5. Plataforma de Gestão de Vulnerabilidade em Ativos de Rede e Nuvem.

1.7.5.1. Características Gerais

1.7.5.1.1. A solução deve ser licenciada para realizar varreduras (scans) de vulnerabilidades, avaliação de configuração e conformidade (baseline e compliance) e indícios e padrões de códigos maliciosos conhecidos (malware);

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

1.7.5.1.3. Deve possibilitar, por meio da console, no mínimo 4 (quatro) métodos de escaneamento:

1.7.5.1.3.1. Scan ativo;

1.7.5.1.3.2. Scan com uso de agentes;

1.7.5.1.3.3. Scan passivo;

1.7.5.1.3.4. Scanner em nuvem;

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

1.7.5.1.5. 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;

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

1.7.5.1.7. A solução deve calcular a criticidade e priorização de vulnerabilidades com base nos dados dos ativos, de preferência utilizando algoritmos de inteligência artificial (machine learning);

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

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

1.7.5.1.10. Deve possuir um sistema de busca de informações de um determinado ativo com, no mínimo, as seguintes características:

1.7.5.1.10.1. Por sistema operacional;

1.7.5.1.10.2. Por um determinado software instalado;

1.7.5.1.10.3. Por Ativos impactados.

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

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

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

1.7.5.1.14. Deve ser capaz de fazer a correlação diária de ameaças ativas contra as vulnerabilidades existentes na infraestrutura;

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

1.7.5.1.16. A solução deve possuir conectores para a seguintes plataformas:

1.7.5.1.16.1. Amazon Web Service (AWS);

1.7.5.1.16.2. Microsoft Azure;

1.7.5.1.16.3. Google Cloud Platform;

1.7.5.1.16.4. Oracle Cloud.

1.7.5.1.17. A solução deve ser capaz de produzir relatórios, no mínimo, nos seguintes formatos: PDF, CSV e HTML;

1.7.5.1.18. A solução deve ser capaz de identificar novos hosts no ambiente sem a necessidade de scan;

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

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

1.7.5.1.21. Deve ser possível determinar quais portas estão abertas em determinado ativo;

1.7.5.1.22. Deve ser capaz de guardar no mínimo os seguintes atributos de um ativo:

1.7.5.1.22.1. Endereço IPv4 e IPv6;

1.7.5.1.22.2. Sistema Operacional;

1.7.5.1.22.3. Nome NetBIOS:

1.7.5.1.22.4. FQDN;

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

1.7.5.1.23.1. Bancos de dados;

1.7.5.1.23.2. Hypervisors;

1.7.5.1.23.3. Dispositivos móveis;

1.7.5.1.23.4. Dispositivos de rede;

1.7.5.1.23.5. Endpoints;

1.7.5.1.23.6. Aplicações;

1.7.5.1.24. Deve realizar em tempo real a identificação de informações sensíveis no tráfego de rede do ambiente;

1.7.5.1.25. A solução deve ser capaz de identificar a comunicação de malwares na rede de forma passiva;

1.7.5.1.26. Deve ser capaz de, em tempo real, detectar logins e downloads de arquivos em um compartilhamento de rede;

1.7.5.1.27. A solução deve ser capaz de, em tempo real, detectar logins e downloads de arquivos em um compartilhamento de rede sem a necessidade de um agente;

1.7.5.1.28. Permitir identificar vulnerabilidades associadas a servidores de Banco de Dados no tráfego de rede em tempo real sem a necessidade de um agente;

1.7.5.1.29. A solução deve possuir interface para integração com as principais soluções de SIEM de mercado, tais como IBM QRadar, Microfocus ArcSight e Splunk;

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

1.7.5.1.31. A solução deve ser capaz de realizar varreduras (scans) de vulnerabilidades para o número de ativos contratados;

1.7.5.1.32. A solução deve ser licenciada para uso de agentes instalados em estações de trabalho e servidores, para varredura diretamente no sistema operacional, no número total de ativos contratados.

1.7.5.1.33. A solução deve realizar varreduras em uma variedade de sistemas operacionais, incluindo no mínimo Windows, Linux e Mac OS, bem como Hypervisors VMWare e Dispositivos de Rede;

1.7.5.1.34. A solução deve suportar vários mecanismos de varredura distribuídos em diferentes localidades e regiões e gerenciar todos por uma console central;

1.7.5.1.35. A solução deve fornecer agentes prontos para instalação em sistemas operacionais distintos, para monitoramento de configurações e vulnerabilidades;

1.7.5.1.36. A solução deve incluir possibilidade de gerenciamento de varreduras: execução, agendamento, exceções, frequências, horários e periodicidade.

1.7.5.1.37. A solução 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;

1.7.5.1.38. A solução deve fornecer a capacidade de escalar privilégios nos destinos, do acesso de usuário padrão até acesso de sistema ou administrativo;

1.7.5.1.39. A solução deverá apresentar o status da vulnerabilidade, demonstrando na interface de gerenciamento se a mesma é Nova, Persistente, Corrigida ou Reincidente no ativo

1.7.5.1.40. Deverá ser possível modificar a severidade das vulnerabilidades, de um único ativo ou múltiplos ativos;

1.7.5.1.41. A solução deve suportar o uso de Tags nos ativos, sendo estas aplicados de forma manual ou automática;

1.7.5.1.42. Deverá ser possível configurar quais usuários, ou grupos de usuários, podem editar as Tags;

1.7.5.1.43. A solução deverá usar as Tags como filtros, podendo ser utilizadas na lista de vulnerabilidades, onde o objetivo é ver todas as vulnerabilidades existentes nos ativos que possuem determinada Tag;

1.7.5.1.44. Ser possível fazer análise dos ativos através de Tags, como exemplo todos os Ativos que possuem a Tag Linux;

1.7.6. Controle de Usuários

1.7.6.1. A solução deve suportar RBAC (Role Based Access Control) com no mínimo 3 tipos de usuários pré-definidos;

1.7.6.2. Deve possuir no mínimo um perfil administrador e um perfil somente leitura;

1.7.6.3. Somente servidores da Contratante ou pessoa por ela autorizada poderão ter acesso aos dados da solução;

1.7.6.4. A solução deve permitir a realização de autenticação com duplo fator através de protocolo RADIUS ou outros meios de comunicação;

1.7.6.5. A solução deve permitir, no mínimo, os seguintes métodos de autenticação: Usuário e senha, LDAP e Radius;

1.7.6.6. A solução deve possibilitar a criação de Grupos de Usuários;

1.7.6.7. Deve permitir configurar quais usuários, ou grupos de usuários, tem permissão de visualizar determinados ativos da organização e suas vulnerabilidades, e quais tem permissão de executar análises de vulnerabilidades nesses ativos;

1.7.6.8. Deve possibilitar configurar permissões, por usuário e grupo de usuário, específicas para cada política de análise de vulnerabilidades;

1.7.7. Relatórios e Dashboards

1.7.7.1. A solução deve suportar o envio automático de relatórios para destinatários específicos;

1.7.7.2. Deve ser possível definir a frequência na geração dos relatórios para, no mínimo: Diário, Mensal e Semanal;

1.7.7.3. A solução deve possuir dashboards customizáveis onde o administrador pode criar, editar ou excluir painéis de acordo com a necessidade;

1.7.7.4. Deve possuir ao menos 5 modelos de dashboards já criados, podendo ser customizados;

1.7.7.5. Deve ser possível exportar os dados em HTML, PDF ou CSV;

1.7.7.6. Deve ser possível exportar os gráficos dos dashboards, através da console de gerenciamento, em PDF, PNG ou JPG;

1.7.7.7. Deve ser possível criar um novo Dashboard e definir este como padrão de visualização do usuário, ou seja, o primeiro Dashboard a aparecer na console no acesso;

1.7.7.8. Deve ser possível configurar um filtro permanente no Dashboards para apresentar informações de todos os ativos, ou somente ativos específicos do ambiente;

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

1.7.7.9.1. Hosts verificados sem credenciais;

1.7.7.9.2. Top 100 Vulnerabilidades mais críticas;

1.7.7.9.3. Top 10 Hosts infectados por Malwares;

1.7.7.9.4. Hosts exploráveis por Malwares;

1.7.7.9.5. Total de vulnerabilidades que podem ser exploradas pelo Metasploit;

1.7.7.9.6. Vulnerabilidades críticas e exploráveis;

1.7.7.9.7. Máquinas com vulnerabilidades que podem ser exploradas.

1.7.8. Conformidade

1.7.8.1. A solução deve ser totalmente licenciada para realizar scans de auditoria e compliance;

1.7.8.2. A solução deve ser capaz de realizar auditoria de conformidade sem a necessidade de agente instalado no dispositivo de destino;

1.7.8.3. A solução deve ser licenciada para realizar scans de conformidade e compliance de forma ilimitada;

1.7.8.4. Toda a solução deve ser licenciada de modo a realizar scans de conformidade para os seguintes padrões: CIS, SCAP e OVAL;

1.7.8.5. A solução deverá possuir modelos prontos de padrões de configuração, no mínimo para: CIS, DISA e MSCT (Microsoft Security Compliance Toolkit)

1.7.8.6. Deve suportar a verificação de compliance para, no mínimo:

1.7.8.6.1. Bluecoat ProxySG;

1.7.8.6.2. Brocade Fabric OS;

1.7.8.6.3. Checkpoint;

1.7.8.6.4. Cisco IOS;

1.7.8.6.5. Citrix Xenserver;

1.7.8.6.6. Fireeye;

1.7.8.6.7. Fortinet FortiOS;

1.7.8.6.8. IBM iSeries;

1.7.8.6.9. Netapp Data ONTAP;

1.7.8.6.10. Palo Alto Firewall;

1.7.8.6.11. Red Hat Enterprise Virtualization;

1.7.8.6.12. Unix;

1.7.8.6.13. Windows;

1.7.8.6.14. VMware.

1.7.8.7. A solução deve gerar um score que combine dados de vulnerabilidades com a criticidade dos ativos do ambiente computacional;

1.7.8.8. O score deve ser gerado automaticamente por meio de algoritmos de inteligência artificial (Machine Learning) e deve calcular a probabilidade de exploração de uma determinada vulnerabilidade;

1.7.8.9. Deve ser capaz de calcular a criticidade dos ativos da organização;

1.7.8.10. Deve fornecer uma lista com as principais recomendações para o ambiente com foco na redução da exposição cibernética da organização;

1.7.8.11. A solução deve gerar uma pontuação para cada um dos ativos, onde é levada em conta as vulnerabilidades presentes naquele ativo, assim como a classificação do ativo na rede (peso do ativo).

1.7.8.12. A solução deve gerar uma pontuação global referente a exposição cibernética da organização baseado nas pontuações de cada um dos ativos.

1.7.8.13. A solução deve permitir um acompanhamento histórico do nível de exposição da organização;

1.7.8.14. Permitir realizar alterações na classificação dos ativos (atribuição de pesos diferentes) podendo sobrescrever a classificação atribuída automaticamente pela solução.

1.7.8.15. A solução deve possuir um gráfico indicativo do percentual de ativos com soluções de proteção de endpoint instaladas, bem como o nome e a versão da solução.

1.7.8.16. A solução deve permitir a segregação lógica entre áreas distintas da empresa a fim de obter a pontuação referente à exposição cibernética por área.

1.7.8.17. A solução deve permitir a segregação lógica entre aplicações distintas da empresa a fim de obter a pontuação referente à exposição cibernética por aplicação.

1.7.9. Plataforma de Gestão de Vulnerabilidade em Aplicações Web

1.7.9.1. Características Gerais

1.7.9.1.1. A solução de gestão de vulnerabilidades deve ser capaz de analisar, testar e reportar falhas de segurança em aplicações Web como parte dos ativos a serem inspecionados;

1.7.9.1.2. A solução deverá ser capaz de executar varreduras em sistemas web através de seus endereços FQDN (DNS);

1.7.9.1.3. Deve possuir modelos (templates) prontos de varreduras e também ser possível a criação de modelos customizados;

1.7.9.1.4. Para varreduras extensas e detalhadas, deve varrer e auditar no mínimo os seguintes elementos:

1.7.9.1.4.1. Cookies, Headers, Formulários e Links;

1.7.9.1.4.2. Nomes e valores de parâmetros da aplicação;

1.7.9.1.4.3. Elementos JSON e XML;

1.7.9.1.4.4. Elementos DOM.

1.7.9.1.5. Deve ser capaz de excluir determinadas URLs da varredura através de expressões regulares;

1.7.9.1.6. Deve ser capaz de excluir determinados tipos de arquivos através de suas extensões;

1.7.9.1.7. Deve ser capaz de instituir no mínimo os seguintes limites:

1.7.9.1.7.1. Número máximo de URLs para crawl e navegação;

1.7.9.1.7.2. Número máximo de diretórios para varreduras;

1.7.9.1.7.3. Número máximo de profundidade dos elementos DOM;

1.7.9.1.7.4. Tamanho máximo de respostas;

1.7.9.1.7.5. Limite de requisições de redirecionamentos;

1.7.9.1.7.6. Tempo máximo para a varredura;

1.7.9.1.7.7. Número máximo de conexões HTTP ao servidor hospedando a aplicação Web;

1.7.9.1.7.8. Número máximo de requisições HTTP por segundo.

1.7.9.1.8. A solução deve ser capaz de detectar congestionamento de rede e limitar os seguintes aspectos da varredura:

1.7.9.1.8.1. Limite em segundos para timeout de requisições de rede;

1.7.9.1.8.2. Número máximo de timeouts antes que a varredura seja abortada.

1.7.9.1.9. Deve ser capaz de agendar a varredura e determinar sua frequência entre: única, diária, semanal, e mensal;

1.7.9.1.10. Deve ser capaz de enviar notificações através de E-mail e, caso possível, outras formas;

1.7.9.1.11. Deverá avaliar sistemas web utilizando frameworks como AJAX, HTML5 e SPA;

1.7.9.1.12. Deverá possibilitar a definição de atributos no cabeçalho (HEADER) da requisição HTTP de forma personalizada a ser enviada durante os testes;

1.7.9.1.13. Deverá ser compatível com avaliação de RESTful APIs;

1.7.9.1.14. Deverá suportar no mínimo os seguintes esquemas de autenticação:

1.7.9.1.14.1. Autenticação básica (digest);

1.7.9.1.14.2. NTLM;

1.7.9.1.14.3. Form de login;

1.7.9.1.14.4. Autenticação de Cookies;

1.7.9.1.14.5. Autenticação através de Selenium.

1.7.9.1.15. Deve ser capaz de importar scripts de autenticação selenium previamente configurados pelo usuário;

1.7.9.1.16. Deve ser capaz de customizar parâmetros Selenium como delay de exibição da página, delay de execução de comandos e delay de comandos para recepção de novos comandos;

1.7.9.1.17. Deve ser capaz de exibir os resultados das varreduras em dashboard dedicados para este tipo de análise;

1.7.9.1.18. Os resultados devem ser apresentados agregados por vulnerabilidades ou por aplicações;

1.7.9.1.19. Para cada vulnerabilidade encontrada, devem ser exibidas as evidências da mesma em seus detalhes;

1.7.9.1.20. Para vulnerabilidades de injeção de código (SQL, XSS, XSRF, etc), deve evidenciar nos detalhes do evento encontrado:

1.7.9.1.20.1. Payload injetado;

1.7.9.1.20.2. Evidência em forma de resposta da aplicação;

1.7.9.1.20.3. Detalhes da requisição HTTP;

1.7.9.1.20.4. Detalhes da resposta HTTP.

1.7.9.1.21. Os detalhes das vulnerabilidades devem conter descrição da falha e referências didáticas para a revisão dos analistas;

1.7.9.1.22. Cada vulnerabilidade encontrada deve conter também soluções propostas para mitigação ou remediação das mesmas;

1.7.9.1.23. A solução deve possuir suporte a varreduras de componentes para, no mínimo:

1.7.9.1.23.1. Wordpress;

1.7.9.1.23.2. AngularJS;

1.7.9.1.23.3. Apache;

1.7.9.1.23.4. Apache Tomcat;

1.7.9.1.23.5. Backbone.js;

1.7.9.1.23.6. ASP.NET;

1.7.9.1.23.7. Bootstrap;

1.7.9.1.23.8. Drupal;

1.7.9.1.23.9. Joomla!;

1.7.9.1.23.10. jQuery;

1.7.9.1.23.11. Magento;

1.7.9.1.23.12. Nginx;

1.7.9.1.23.13. PHP; e

1.7.9.1.23.14. AJAX.

1.7.9.1.24. A solução deverá possuir controle de permissão de usuários, com no mínimo ,3 níveis, sendo: Administrador, Operador de Scan e Somente Leitura;

1.7.9.1.25. Deverá possuir a capacidade de manter privado os resultados de um scan, ou seja, não aparecendo o resultado no dashboard da solução;

1.7.9.1.26. A solução poderá possuir scanners pré-configurados em nuvem, para realização de scans externos;

1.7.9.1.27. A solução deve possuir, também, sensores (scanner) on-premisses;

1.7.9.1.28. Deverá ser possível exportar os gráficos do dashboard em PDF, PNG ou JPEG, nativamente pelo console de gerência.

1.7.9.1.29. A solução deve suportar listas de exclusão globais;

1.7.9.1.30. Deve possuir um dicionário já criado com as principais páginas comuns e páginas de backup existentes.

1.7.9.1.31. Deve apresentar a nota do CVSSv3 nas vulnerabilidades encontradas;

1.7.9.1.32. A solução deverá gerar relatórios das vulnerabilidades, no mínimo em PDF, HTML e CSV.

1.7.10.1. Características Gerais

1.7.10.1.1. A solução deverá ser licenciada contabilizando o número de imagens únicas, não sendo contabilizadas novas versões de uma mesma imagem;

1.7.10.1.2. A solução de gestão de vulnerabilidades deve ser capaz de analisar, testar e reportar falhas de segurança em aplicações em Containers Docker como parte dos ativos a serem inspecionados;

1.7.10.1.3. A solução deve ser capaz de analisar imagens em Container utilizadas pelo TRT12, preparadas pelos desenvolvedores, em busca de vulnerabilidades identificadas e malwares residentes no sistema de arquivos;

1.7.10.1.4. A documentação de API da solução deverá ter acesso público através de website ou documentação do próprio fabricante;

1.7.10.1.5. A console de administração deverá possuir controle de acesso no mínimo permitindo usuários com capacidade de somente visualizar as informações, e usuários com capacidade para efetuar análise das imagens;

1.7.10.1.6. A solução deve inventariar o sistema operacional de cada imagem analisada e suas vulnerabilidades encontradas;

1.7.10.1.7. A solução deve ser capaz de identificar containers que não foram analisados antes de sua implementação em produção;

1.7.10.1.8. A solução deve analisar as camadas (layers) de um container;

1.7.10.1.9. A solução deve ser capaz de identificar containers que tiveram mudanças de arquivos entre a análise e a sua implementação em produção;

1.7.10.1.10. A solução deve ser capaz de identificar as devidas tags das imagens avaliadas;

1.7.10.1.11. A solução deve informar os CVEs para cada vulnerabilidade encontrada nos pacotes e bibliotecas residentes na imagem;

1.7.10.1.12. A solução deve ter a capacidade de testar automaticamente todas as imagens armazenadas, ou previamente testadas, sempre que uma nova vulnerabilidade for publicada e atualizada no banco de dados de vulnerabilidade da solução, sem qualquer tipo intervenção manual;

1.7.10.1.13. Deve ser capaz de inventariar os pacotes e bibliotecas e suas respectivas versões;

1.7.10.1.14. A solução deve possuir conectores e permitir importação de imagens, no mínimo, dos seguintes repositórios:

1.7.10.1.14.1. Docker HUB;

1.7.10.1.14.2. GitLab Container Registry;

1.7.10.1.14.3. Harbor;

1.7.10.1.14.4. Oracle Container Registry.

1.7.10.1.15. A solução deve fornecer scanner em formato Docker para implementação local e análise de imagens sem a necessidade de envio destas para repositório remoto, fora do ambiente da CONTRATANTE;

1.7.10.1.16. A solução ser capaz de configurar políticas usando como condições: CVSS Score, CVEs específicos e Malware identificado;

1.7.10.1.17. A solução deve permitir a criação de políticas específicas por repositório;

1.7.10.1.18. A solução deve prover integração com, no mínimo, as seguintes plataformas de integração contínua: GitLab, Jenkins, Argo CD, Travis CI e Kubernetes;

1.7.10.1.19. A solução deverá ser capaz de analisar vulnerabilidades também na infraestrutura, onde as imagens de container são executadas, tanto do sistema operacional quanto das aplicações que nele estão instaladas. Esta capacidade poderá ser:

1.7.10.1.19.1. Nativa da solução, desde que exista uma extensa compatibilidade de sistemas operacionais e aplicações relacionadas a

container, algumas já explicitadas em itens anteriores, e já licenciada para uso;

1.7.10.1.19.2. Executada através de integração com terceiros, desde que toda a solução esteja licenciada para a CONTRATANTE;

1.7.11. Suporte Técnico Especializado.

1.7.11.1. A CONTRATADA deverá fornecer serviços de manutenção e suporte técnico pelo período de 60 (sessenta) meses, contados da data da assinatura do contrato de suporte técnico especializado, contemplando o suporte técnico para os sistemas e/ou appliances que compõem a Solução de Gerenciamento de Vulnerabilidades;

1.7.11.2. A CONTRATADA deverá prestar serviço de manutenção e suporte técnico destinado a:

1.7.11.2.1. Restabelecimento de serviços interrompidos ou degradados;

1.7.11.2.2. Solução de problemas de configuração e falhas técnicas nos serviços;

1.7.11.2.3. Esclarecimentos de dúvidas sobre configurações e utilização dos serviços;

1.7.11.2.4. Implementação de novas funcionalidades.

1.7.11.2.5. Entre outras situações correlatas às acima exemplificadas;

1.7.11.3. A CONTRATADA deverá atender as seguintes premissas:

1.7.11.3.1. Os serviços serão solicitados mediante a abertura de chamados a serem efetuados por técnicos do Tribunal, via chamada telefônica local ou gratuita, e-mail ou website, sem custos para a CONTRATANTE.

1.7.11.3.2. Não haverá limitação de quantidade de abertura de chamados para suporte.

1.7.11.3.3. O suporte deve estar disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, nos 365 (trezentos e sessenta dias) do ano, sendo o Português Brasileiro o idioma de suporte técnico obrigatório.

1.7.11.3.4. Os serviços de suporte deverão ser prestados por técnicos devidamente capacitados nos respectivos componentes da solução. Caberá à CONTRATADA fornecer aos seus técnicos todas as ferramentas e os instrumentos necessários à execução dos serviços.

1.7.11.3.5. Todas as solicitações feitas pelo CONTRATANTE deverão ser registradas pela CONTRATADA em sistema informatizado para acompanhamento e controle da execução dos serviços.

1.7.11.3.6. O acompanhamento da prestação de serviço deverá ser através de um número de protocolo fornecido pela CONTRATADA, no momento da abertura da solicitação.

1.7.11.3.7. Requisitos de Atendimento:

1.7.11.3.7.1. A CONTRATADA deverá realizar, mensalmente, procedimento de health check (check up) das configurações da(s) ferramenta(s) que façam parte da solução, propondo as melhorias necessárias através de relatórios, baseando-se nas boas práticas recomendadas pelo fabricante;

1.7.11.3.7.2. A CONTRATADA deve emitir, mensalmente, relatórios de vulnerabilidades e proposições de melhorias, no contexto da solução contratada, para avaliação do CONTRATANTE:

1.7.11.3.7.2.1. Procedimentos de correção e/ou contramedidas recomendadas pela equipe especializada da Contratada;

1.7.11.3.7.2.2. Orientações para o System Hardening dos serviços, servidores, elementos ativos e aplicações avaliados;

1.7.11.3.7.2.3. Sugestão para incremento da segurança e proteção do ambiente;

1.7.11.3.7.2.4. Os relatórios devem ser entregues em português, podendo os anexos técnicos possuírem dados em língua inglesa.

1.7.11.3.7.3. A CONTRATADA deve comunicar formalmente o CONTRATANTE sempre que identificar algum serviço com falhas de implementação e que tornem o ambiente vulnerável a indisponibilidade, bem como a realização permanente de ações proativas voltadas ao incremento da segurança do parque computacional do TRT12, a fim de mantê-lo estável, disponível e íntegro.

1.7.11.3.7.4. A CONTRATADA deverá apoiar o CONTRATANTE em caso de mudanças requeridas por conta de atualizações ou remanejamentos de infraestrutura, quando tais alterações envolver a solução ora contratada;

1.7.11.3.7.5. A CONTRATADA deverá realizar, no contexto da solução contratada, sob autorização e supervisão da CONTRATADA: instalação de softwares, acompanhamento de migrações de regras e políticas, elaboração e execução de scripts, análise de performance, resolução de problemas e implementação de segurança.

1.7.11.3.7.6. Os relatórios produzidos devem ser apresentados e discutidos em reunião mensal, com presença de profissional que conheça todos os serviços. Nesse contexto, o profissional deve apresentá-lo de forma presencial nas dependências do CONTRATANTE ou de forma virtual, por meio de solução de videoconferência de preferência do CONTRATANTE.

1.7.11.3.7.7. Não serão aceitos relatórios obtidos diretamente de ferramentas automatizadas utilizadas, sem a devida transcrição e contextualização adequada com o ambiente do TRT12.

1.7.11.3.8. Dos prazos de atendimento:

1.7.11.3.8.1. A tabela abaixo descreve os prazos de atendimento que deverão ser cumpridos pela CONTRATADA, de acordo com a severidade de cada chamado aberto:

Tabela de Solução dos chamados			
Severidade	Descrição	Tempo para primeiro contato após abertura do chamado	Tempo de resolução do chamado
Urgente	Serviço crítico parado em produção.	30 minutos	Até 01 (uma) hora
Alta	Erros e problemas que estão impactando no ambiente de produção.	60 minutos	Até 04 (quatro) hora
Média	Problemas ou erros contornáveis que afetam o ambiente em produção, mas não possuem alto impacto.	90 minutos	Até 06 (seis) horas
Baixa	Problemas ou erros contornáveis que não impactam significativamente no ambiente em produção.	120 minutos	Até 08 (oito) horas
Informações	Consulta Técnica, dúvidas em geral, monitoramento.	150 minutos	Até 24 (vinte e quatro) horas

1.7.11.3.8.2. O prazo de atendimento deve começar a ser contabilizado a partir do momento de efetivação da abertura do suporte, através de telefone ou e-mail;

1.7.11.3.9. A CONTRATADA deve apresentar relatório de visita para cada solicitação de suporte on-site, contendo a data e hora da solicitação de suporte técnico, o início e o término do atendimento, identificação do problema, providências adotadas e demais informações pertinentes;

1.7.11.3.10. O nível de severidade será informado no momento da abertura de cada chamado pelo técnico responsável do CONTRATANTE;

1.7.11.3.11. Todas as solicitações de suporte técnico devem ser registradas pela CONTRATADA para acompanhar e controlar a execução dos chamados;

1.7.11.3.12. O descumprimento dos prazos de atendimento implicará na aplicação de glosas conforme tabela abaixo:

Tabela de aplicação de Glosas		
Severidade	Fórmula de cálculo da glosa	Limite da glosa
Urgente	HS x 0,5% * VFM	20% da VFM
Alta	HS x 0,4% * VFM	15% da VFM
Média	HS x 0,3% * VFM	10% da VFM
Baixa	HS x 0,2% * VFM	10% da VFM
Informações	HS x 0,1% * VFM	10% da VFM
HS = Horas totais que extrapolaram o limite de resolução dos chamados, no caso de hora quebrada, será apurado o percentual da hora descumprida.		
VFM = Valor da Fatura Mensal para pagamento do serviço de suporte.		
Em caso de descumprimento contumaz pela CONTRATADA nos prazos para atendimento do suporte técnico a fiscalização poderá adotar a aplicação de sanções: advertências, multas, suspensão temporária de participação em licitação e impedimento de contratar com a Administração e declaração de inidoneidade para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, na forma da lei 8.666, de 1993.		

1.7.11.3.13. A CONTRATADA deve emitir relatório mensal em arquivo eletrônico ou em sistema de consulta online, com informações dos chamados abertos e fechados no período;

1.7.11.3.14. O relatório deve possuir os seguintes parâmetros:

1.7.11.3.14.1. Quantidade de ocorrências (chamados) registradas no período;

1.7.11.3.14.2. Número do chamado registrado e nível de severidade;

1.7.11.3.14.3. Data e hora de abertura;

1.7.11.3.14.4. Data e hora de início e conclusão do atendimento;

1.7.11.3.14.5. Identificação do técnico que fez o registro do chamado;

1.7.11.3.14.6. Descrição do problema;

1.7.11.3.14.7. Descrição da solução;

1.7.11.3.15. Problemas cuja solução dependa de correção de falhas (bugs) ou da liberação de novas versões e patches de correção, desde que comprovados pelo fabricante da solução, não deverão se encaixar nos prazos estabelecidos acima;

1.7.11.3.16. A CONTRATADA deverá, de acordo com o nível de criticidade, prover solução paliativa para atender os problemas de falhas (bugs), atualizações ou patches de correção que ainda não foram disponibilizadas pela fabricante, no prazo de 24 (vinte e quatro) horas, para restabelecer o ambiente do CONTRATANTE;

1.7.11.3.17. A solução definitiva deverá ser disponibilizada no prazo máximo de 60 (sessenta) dias, sendo a CONTRATADA responsável pelos trâmites juntamente a fabricante da liberação das correções.

1.7.11.3.18. Nas manutenções que necessitem de intervenção para parada física ou reinicialização do equipamento, o CONTRATANTE deverá ser notificado previamente para que faça o agendamento da manutenção e aprovação;

1.7.11.3.19. As paradas de manutenção deverão acontecer fora do horário de expediente, de preferência após a 20 (vinte) horas devendo ser restabelecida antes das 8 (oito) horas da manhã do dia seguinte. Poderá ocorrer durante o dia da semana ou aos finais de semana, sem ônus para o CONTRATANTE;

1.7.11.3.19.1. Todo o procedimento de manutenção deverá ser documentado, explicando o passo a passo completo e fazendo registro das ocorrências incoerentes para subsidiar novas paradas que possam acontecer;

1.7.11.3.19.2. O relatório deverá ser assinado pelo fiscal técnico do contrato ou responsável pelo acompanhamento do serviço por parte do CONTRATANTE.

1.7.12. Treinamento técnico da Solução de Gerenciamento de vulnerabilidades.

1.7.12.1. O treinamento técnico da Solução de Gerenciamento de Vulnerabilidades será de, no mínimo, 40 horas, para turma de, no máximo, 10 alunos;

1.7.12.2. O treinamento, ou parte dele, poderá ser realizado no modelo telepresencial (online por videoconferência), em português, utilizando ferramenta própria disponibilizada pelo contratado (ex.: Microsoft Teams, Cisco Webex, Google Meet, etc.), desde que autorizado pelo Contratante;

1.7.12.3. O Contratante disponibilizará os computadores a serem utilizados pelos participantes do curso;

1.7.12.4. A CONTRATADA disponibilizará material didático oficial do curso em formato digital (PDF) aos participantes e quaisquer conteúdos e ferramentas adicionais que venham a ser necessárias para o treinamento;

1.7.12.5. Caso não haja disponibilidade para realização nos modelos presencial ou telepresencial, a Contratada custeará os gastos de passagens e estadia para o centro de treinamento mais próximo de Belém.

1.7.12.6. O treinamento deverá ser ministrado em português, por técnico certificado pelo fabricante da solução, e composto de aulas teóricas e práticas.

1.7.12.7. A CONTRATADA deverá confeccionar e disponibilizar aos participantes todo o material didático necessário ao treinamento, de todos os módulos que compõem a Solução.

1.7.12.8. A ementa e material utilizado no treinamento deverão ser enviados previamente ao Tribunal para avaliação e aprovação.

1.7.12.9. O treinamento deverá desenvolver o conhecimento e habilidades necessárias para fazer uso de todos os recursos disponíveis na Solução adquirida, incluindo, principalmente, a identificação dos Ativos de TI, o SCAN de Vulnerabilidades, Análise do SCAN, Avaliação de Riscos, Aplicação de Políticas, Compliance, dentre outras funcionalidades chaves da Solução.

1.7.12.10. Ao final do treinamento, deverá ser realizada junto aos participantes uma avaliação do curso. As avaliações deverão ser preenchidas e assinadas pelos alunos e posteriormente entregues ao Tribunal para a assinatura do aceite da Ordem de Serviço do treinamento.

1.7.12.11. Caso o treinamento seja avaliado como insatisfatório pela maioria dos participantes da turma, o treinamento deverá ser refeito.

1.7.12.12. Será considerado insatisfatório o treinamento que obtiver maioria dos itens da avaliação de treinamento julgados como RUIM ou REGULAR, observadas todas as avaliações preenchidas.

1.7.12.13. O treinamento a ser refeito por ocasião de ter sido mal avaliado não pode gerar novas despesas para o CONTRATANTE.

1.7.12.14. Ao final do treinamento, cada participante deverá receber um certificado assinado pela CONTRATADA, contendo informações de data, carga horária, conteúdo ministrado, além do nome completo do instrutor, do aluno e da instituição que forneceu o curso, bem como o seu período.

1.7.12.15. A Contratada deverá fornecer certificado para cada aluno contendo identificação da instituição que forneceu o treinamento, nome do aluno, local do treinamento, período do treinamento, carga horária, nome do instrutor e conteúdo programático.

1.8. Relação entre a demanda prevista e a quantidade adquirida

O quantitativo planejado para esta contratação consta no item 1.3 deste documento, onde são especificados com crescimento na ordem de 25%, que deverá permitir a conclusão do contrato sem nenhuma intercorrência. Também é possível o rearranjo de licenças para cobrir qualquer crescimento anormal de alguma parte da presente contratação.

1.9. Considerações sobre os preços.

O TRT12 é participante da licitação nacional, da qual resultou a Ata de Registro de Preços Nº 5/2022, Pregão Eletrônico nº 4/2022, gerenciada pelo TRT da 8ª Região, assinada em 16-04-2022.

Preço 1 - MPDFT - Pregão Eletrônico n°062/2020 (marcador 10), (marcador 18 proad 10438/2022), embora fora do prazo estabelecido na portaria PRESI

339/2022, por se tratar de objeto mais próximo do pregão que somos coparticipes, consideramos que este preço deve ser utilizado para compor a cesta de preços. Esta ata engloba os itens 1, 2, 3 e 4, sem existir distinção do tipo de ação, desta forma ele aparece repetido nos quatro itens. Por ter um prazo menor (36 meses) os valores foram calculados de forma mensal e depois acrescentados do período de 60 meses para comparação.

Preço 2 - Tribunal Regional Eleitoral da Paraíba - Pregão Eletrônico n° 037/2020 (marcadores 11, 12 e 13), embora fora do prazo estabelecido na portaria PRESI 339/2022, por se tratar de objeto mais próximo do pregão que somos coparticipes, consideramos que este preço deve ser utilizado para compor a cesta de preços. Por ter um prazo menor (36 meses) os valores foram calculados de forma mensal e depois acrescentados do período de 60 meses para comparação.

Preço 3 - Tribunal De Contas De Roraima - Pregão eletrônico 017/2021 (marcador 14) (marcador 19 proad 10438/2022) - Aquisição de solução unificada de Gestão de Vulnerabilidades em ativos de tecnologia da informação e aplicações web, compreendendo aquisição de serviços de software e suporte técnico, para atender as necessidades do tribunal de contas do estado por 36 (trinta e seis) meses, por ter um prazo menor os valores foram calculados de forma mensal e depois acrescentados do período de 60 meses para comparação.

Preço 5 - Base Administrativa Do Centro De Comunicações E Guerra Eletrônica Do Exército Pregão Eletrônico No 26/2021, (marcador 15 e 16) - O objeto da presente licitação é a escolha da proposta mais vantajosa para a contratação de serviços de tecnologia da informação e comunicação de licença para utilização de software de análise de vulnerabilidade Tenable Network Security Nessus Professional por 36 (trinta e seis) meses, por ter um prazo menor os valores foram calculados de forma mensal e depois acrescentados do período de 60 meses para comparação.

Solicitamos ainda as empresas Servix e Teletex que fornecessem preço para comparação da Ata, contudo passado mais de um mês ainda não obtivemos

resposta dessas empresas, o que geralmente se deve ao fato dessas empresas saberem que somos coparticipantes de uma licitação e que não vão conseguir fazer uma proposta melhor do que o pregão que participamos. Segue nos marcadores 17 e 18 os emails solicitando preços.

O Pregão do Ministério Público do Estado da Bahia - Pregão Eletrônico No 04/2022 - (marcador 19), foi desconsiderado pois o mesmo foi suspenso.

Para entendimento da tabela a seguir foi pego o valor total dividido pela duração do contrato e o resultado dividido pela quantidade obtendo assim o valor unitário da solução, para os itens de 1 a 4.

ITEM	ESPECIFICAÇÃO	VALOR UNITÁRIO R$	QTDE	Duração	ÓRGÃO / PROPOSTA	VALOR TOTAL R$
1	Solução de Gerenciamento de vulnerabilidades para FQDNs Externos, dos ativos de Tecnologia da Informação, baseada e com análise contínua e adaptável de riscos e confiança, com o serviço de implantação e também o de garantia dos equipamentos e/ou softwares pelo período de 60 meses.	21,95	1031	36 meses	MPDFT - Pregão Eletrônico n°062/2020 item 1	814.490,00
		512,60*	5	36 meses	Tribunal Regional Eleitoral da Paraíba - Pregão Eletrônico n° 037/2020	92.268,00*
		250,99*	10	36 meses	TCERR Pregão Eletrônico n° 17/2021- item 2	90.357,00*
	Média item 1	**21,95**				
2	Solução de Gerenciamento de vulnerabilidades para FQDNs Internos, dos ativos de Tecnologia da Informação, baseada e com análise contínua e adaptável de riscos e confiança, com o serviço de implantação e também o de garantia dos equipamentos e/ou softwares pelo período de 60 meses.	**365,80***	10	36 meses	Tribunal Regional Eleitoral da Paraíba - Pregão Eletrônico n° 037/2020	131.686,00*
		21,82	128	36 meses	TCERR Pregão Eletrônico n° 17/2021- item 1	100.548,33
		21,95	1031	36 meses	MPDFT - Pregão Eletrônico n°062/2020 item 1	814.490,00
	Média item 2	**21,88**				

3	Solução de Gerenciamento de vulnerabilidades para Imagens de aplicações em Container, baseada e com análise contínua e adaptável de riscos e confiança, com o serviço de implantação e também o de garantia dos equipamentos e/ou softwares pelo período de 60 meses.	18,72	500	36 meses	Tribunal Regional Eleitoral da Paraíba - Pregão Eletrônico n° 037/2020	337.000,00
		21,95	1031		MPDFT - Pregão Eletrônico n°062/2020 item 1	814.490,00
	Média item 3	**20,34**				
4	Solução de Gerenciamento de vulnerabilidades para Endpoints, baseada e com análise contínua e adaptável de riscos e confiança, com o serviço de implantação e também o de garantia dos equipamentos e/ou softwares pelo período de 60 meses.	21,95	1031	36 meses	MPDFT - Pregão Eletrônico n°062/2020 item 1	814.490,00
		40,70*	256	36 meses	CCOMGEX	375.000,00*
	Média item 4	**21,95**				
5	Suporte técnico especializado.	**1.300,00**				
			4 horas		Tribunal Regional Eleitoral da Paraíba - Pregão Eletrônico n° 037/2020	1.250,00
			4 horas		TCERR Pregão Eletrônico n° 17/2021- item 5	1.350,00
6	Treinamento técnico da Solução de Gerenciamento de vulnerabilidades.	**5.663,33**	1		MPDFT - Pregão Eletrônico n°062/2020**	4.400,00
			1		Tribunal Regional Eleitoral da Paraíba - Pregão Eletrônico n° 037/2020	8.340,00
			1		TCERR Pregão Eletrônico n° 17/2021- item 4**	4.250,00

Os valores marcados com (*) foram retirados da cesta de preços pois apresentam valores muito fora da pesquisa e comprometem a fidedignidade do levantamento. Os cursos marcados com (**) são cursos de 20 horas.

Conforme mencionado anteriormente os contratos listados acima são todos contratos de 36 meses já o pregão realizado pelo TRT 08 é de 60 meses.

Abaixo segue tabela com valores da Ata de Registro de Preço 05/2022 do TRT 08, também calculado com os valores totais da referida ata dividindo pelo número de meses e o resultado novamente dividido pela quantidade da ata:

Tabela comparativa				
Item	**Especificação**	**VALOR UNITÁRIO R$**	**VALOR UNITÁRIO R$ Ata TRT08**	**OBS**
1	Solução de Gerenciamento de vulnerabilidades para **FQDNs Externos**, dos ativos de Tecnologia da Informação, baseada e com análise contínua e adaptável de riscos e confiança, com o serviço de implantação e também o de garantia dos equipamentos e/ou softwares pelo período de 60 meses.	**R$ 21,95**	R$ 19,16	
2	Solução de Gerenciamento de vulnerabilidades para **FQDNs Internos**, dos ativos de Tecnologia da Informação, baseada e com análise contínua e adaptável de riscos e confiança, com o serviço de implantação e também o de garantia dos equipamentos e/ou softwares pelo período de 60 meses.	**R$ 21,88**	R$18,58	
3	Solução de Gerenciamento de vulnerabilidades para **Imagens de aplicações em Container**, baseada e com análise contínua e adaptável de riscos e confiança, com o serviço de implantação e também o de garantia dos equipamentos e/ou softwares pelo período de 60 meses.	**R$ 20,34**	R$ 20,06	
4	Solução de Gerenciamento de vulnerabilidades para **Endpoints**, baseada e com análise contínua e adaptável de riscos e confiança, com o serviço de implantação e também o de garantia dos equipamentos e/ou softwares pelo período de 60 meses.	**R$ 21,95**	R$ 24,21	1
5	Suporte técnico especializado.	**R$ 1.300,00**	R$ 10.000,00	2
6	Treinamento técnico da Solução de Gerenciamento de vulnerabilidades.	**R$ 5.663,33**	R$ 8.600	3

Podemos verificar que os preços obtidos na Ata de Registro de Preços Nº

5/2022, gerenciada pelo TRT da 8ª Região, se mantêm dentro dos valores de mercado. Podemos notar também um certo jogo nos valores como o Pregão do TRE e do TCE que gerou algumas distorções nos preços, mas nada que invalide a pesquisa, uma vez que foram descartados. Nota-se na obs1 que o valor do Pregão do TRT 08 ficou um pouco acima da média, mas não o suficiente para invalidar a escolha.

Quanto a obs 2, o valor ficou acima, pois nas duas pesquisas de preços encontradas, os órgãos estão contratando pacotes de 4 horas de suporte, enquanto o pregão do TRT 08 está contratando um pacote de atendimento 24h x 07 dias, desta feita o suporte contratado é muito superior ao levantado na pesquisa. Como podemos verificar no seguinte calculo 24 horas vezes 30 dias da 720 horas, dividindo R$ 10.000,00 por 720 temos R$ 14,00 por hora vezes 4 horas o pacote sai por R$55,55 um custo muito abaixo.

Em relação a obs 3, o treinamento contratado nas pesquisas é com carga horária mínima de 20 horas, sendo que no pregão do MPDF nem previsão de horas possui nas especificações, já o do Pregão do TRT 08 é de 40 horas. Ou seja se dobrarmos o custo das pesquisas para ter um curso de 40 horas, teremos o mesmo custo do que foi levantado na licitação do TRT 08.

Desta forma a equipe da contratação opta por aderir a Ata de Registro de Preços Nº 5/2022 do TRT da 8ª Região

1.10 Avaliação das necessidades de adequação do ambiente para viabilizar a execução contratual.

Item	Característica	O que precisa ser feito	Responsável
01	Infraestrutura tecnológica (equipamentos, redes, link, etc..)	Não há necessidade de instalação de equipamentos da solução adquirida no datacenter principal do TRT12.	
02	Infraestrutura elétrica	Não há necessidade de adequação da infraestrutura elétrica	
03	Logística de implantação	Não haverá necessidade de deslocamento da equipe da SEGINFO.	Equipe da SEGINFO
04	Espaço Físico	Nenhum dos equipamentos previstos na demanda necessitarão de adequação do espaço físico para seu funcionamento.	

05	Mobiliário	Não há necessidade de adequação do mobiliário	
06	Impacto ambiental	Não haverá impacto ambiental.	
07	Liberação de acesso	Permissões de acesso a funcionários da contratada para fazer a instalação nas dependências do tribunal.	Equipe da SEGINFO
08	Outros	Não há conhecimento de outras necessidades de adequação além das já comentadas	

1.11. Disponibilidade Orçamentária

Demanda prevista nos itens 15907, 15908 e 15909 do PAC. Os recursos previstos para viabilizar a execução contratual serão descentralizados pelo CSJT.

O valor estimado para a contratação é de R$ 2.576.100,00 no orçamento de 2022, sendo:

- Custeio - GND3: R$ 81.600,00
  - Item 5 - Suporte técnico especializado - 3 meses - Valor mensal R$ 10.000,00, Valor Total para 2022 R$: 30.000,00;
  - Item 6 - Treinamento técnico da Solução de Gerenciamento de vulnerabilidades - 6 unidades, Valor Total: R$ 51.600,00 ;
- Investimento - GND4: R$ 2.484.500,00 - Itens 1, 2, 3 e 4 (que garantirão a sustentação das licenças até 2027).

Para os próximos exercícios financeiros deverão ser previstos os valores para pagamento do Item 5 - Suporte técnico especializado (Valor mensal R$ 10.000,00).

2. Capítulo II - SUSTENTAÇÃO DO CONTRATO

2.1. Recursos Necessários à Continuidade do Negócio Durante e Após a Execução do Contrato

2.1.1. Recursos Materiais

2.1.1.1. Recurso 1: Ambiente de Virtualização **- Responsável:** Responsável pela

área de Infraestrutura de TIC.

- Ação para Obtenção do Recurso: Recurso já está disponível;

- Responsável: Responsável pela área de Infraestrutura de TIC.

2.1.2. Recursos Humanos

Os recursos humanos para viabilizar o gerenciamento e fiscalização da solução serão os servidores do quadro permanente do TRT12 lotados no Serviço de Infraestrutura de TIC (SEINFRA) e Divisão de Segurança da Informação e Proteção de Dados (SEGINFO). Já a equipe de técnicos especialistas necessários para instalação, suporte e treinamento da solução são de responsabilidade da contratada.

2.2. Estratégia de Continuidade Contratual

Para o caso de interrupção contratual por problemas com fornecedores antes da entrega/atualização dos produtos, o gestor do contrato deve informar à administração do Tribunal para a aplicação das sanções previstas.

2.3. Ações de transição e encerramento contratual

Caso não haja intercorrências, o encerramento do contrato irá restringir o acesso do Tribunal ao objeto da contratação.

Permanecendo a necessidade de uso do produto, o gestor do contrato deverá protocolar nova demanda para aquisição até 90 (noventa) dias antes do encerramento do contrato.

2.3.1. Entrega das versões finais dos produtos

A contratada deve disponibilizar, via site na internet, todas as licenças e manuais dos produtos nas versões mais atuais, do momento do fornecimento até o encerramento da vigência do contrato.

Além disso, a contratada deve fornecer acesso a todas as atualizações que forem produzidas dentro do período do contrato de suporte, independentemente de solicitação do TRT12. Fica a critério do Tribunal, contudo, a instalação dessas

atualizações em seu ambiente computacional, em função dos riscos que possam decorrer da alteração de versões de produção.

2.3.2. Transferência final de conhecimentos

Será de inteira responsabilidade da CONTRATADA, sem ônus adicional para a TRT 12, garantir o repasse bem sucedido de todas as informações necessárias para a continuidade dos serviços pelo TRT 12 ou empresa por este designada, sendo realizado na implantação da solução, durante o treinamento ou na vigência do contrato.

2.3.3. Devolução de recursos materiais

Não é aplicável.

2.3.4. Revogação de perfis de acesso

Todos os eventuais acessos criados para os colaboradores da contratada devem ser formalmente solicitados com descrição detalhada das funções que os trabalhadores executarão. Após o término das atividades, o Tribunal revogará todos os acessos utilizados durante o processo de implantação.

2.4. Estratégia de independência

Existem várias soluções no mercado que atendem os requisitos. A solução a ser contratada é proprietária e não customizada. Pode ser fornecida por pelo menos 4 fornecedores diferentes, porém não há integração entre as soluções. Apenas relatórios, guias de implantação, informações do ambiente e dados extraídos das estações e servidores do TRT 12 serão propriedade do Tribunal. Sendo assim, caso ao fim do contrato o Tribunal opte por mudar de solução, deverá analisar custos, funcionalidades e poderá fazê-lo.

2.4.1. Formas de transferência do conhecimento.

2.4.1.1. A CONTRATADA deverá entregar ao Tribunal toda e qualquer documentação gerada em meio magnético e/ou físico em função da prestação de serviços.

2.4.1.2. As informações geradas pela CONTRATADA estarão disponíveis em ferramentas e em documentos conforme as definições e padrões utilizados pelo Tribunal.

2.4.1.3. Deverá haver transferência de conhecimento da CONTRATADA para o Tribunal em relação às tecnologias utilizadas na prestação de serviços para melhor eficiência, eficácia, efetividade e economicidade com sua adoção.

2.4.1.4. Será de inteira responsabilidade da CONTRATADA, sem ônus adicional para o Tribunal, garantir o repasse bem sucedido de todas as informações necessárias para a continuidade dos serviços pelo órgão ou empresa por este designada.

2.4.1.5. O apoio na fase de implantação, pela transferência técnica, no uso das soluções implantadas pela CONTRATADA, deverá ser viabilizado, sem ônus adicionais para o Tribunal, e baseado em documentos funcionais, técnicos e/ou manuais específicos da solução desenvolvida. O cronograma e horários dos eventos deverão ser previamente aprovados pelo órgão.

2.4.2. Direitos de Propriedade Intelectual (Lei nº 9.610, de 19 de fevereiro de 1998)

Não há previsão de desenvolvimento de qualquer novo conhecimento, código ou outro tipo de conhecimento que se converta em propriedade intelectual.

2.4.3. Outras formas de minimizar dependência

A equipe de fiscalização técnica se manterá atenta à qualidade das entregas para garantia da independência do fornecedor.

3. Capítulo III - ESTRATÉGIA DA CONTRATAÇÃO

3.1. Natureza do objeto

Trata-se de aquisição de serviço comum, cujos padrões de desempenho e qualidade foram objetivamente definidos pelo edital, por meio de especificações usuais no mercado.

3.2. Parcelamento do objeto

Conforme Edital do Pregão Eletrônico nº 4/2022 do TRT da 8ª Região, marcador 20.

3.3. Modalidade e tipo de licitação (justificativa)

Verifica-se que o objeto pretendido é oferecido por alguns fornecedores no mercado de TIC, e apresenta características padronizadas e usuais. Assim, pode-se concluir que o objeto é comum e, portanto, a melhor opção de modalidade foi a utilizada pelo TRT da 8ª Região: Pregão eletrônico do tipo menor preço.

Esta equipe sugere adesão à Ata de Registro de Preços Nº 5/2022, resultante do Pregão Eletrônico nº 4/2022, gerenciada pelo TRT da 8ª Região.

3.4. Classificação Orçamentária.

Demanda prevista nos itens 15907, 15908 e 15909 do PAC. Os recursos previstos para viabilizar a execução contratual serão descentralizados pelo CSJT.

O valor estimado para a contratação é de R$ 2.576.100,00 no orçamento de 2022, sendo:

- Custeio - GND3: R$ 81.600,00
    - Item 5 - Suporte técnico especializado - 3 meses - Valor mensal R$ 10.000,00, Valor Total para 2022 R$: 30.000,00;
    - Item 6 - Treinamento técnico da Solução de Gerenciamento de vulnerabilidades - 6 unidades, Valor Total: R$ 51.600,00 ;
- Investimento - GND4: R$ 2.484.500,00 - Itens 1, 2, 3 e 4 (que garantirão a sustentação das licenças até 2027).

Para os próximos exercícios financeiros deverão ser previstos os valores para pagamento do Item 5 - Suporte técnico especializado (Valor mensal R$ 10.000,00).

Item 1. Software: 44904005 – Aquisição de Software Pronto.
Item 2. Software: 44904005 – Aquisição de Software Pronto.
Item 3. Software: 44904005 – Aquisição de Software Pronto.
Item 4. Software: 44904005 – Aquisição de Software Pronto.
Item 5. Suporte Técnico: 33904021 - Serviços Técnicos de Profissionais de TIC
Item 6. Treinamento: 33904020 – Treinamento / Capacitação em TIC.

3.6. Equipe de apoio à contratação

Este papel será desempenhado pela equipe de planejamento da contratação.

3.7. Equipe de gestão da contratação

a) Gestor do Contrato e Fiscal Demandante: Serão indicados nominalmente pelo Diretor da Secretaria demandante. A indicação será efetuada no despacho de aprovação dos Estudos Preliminares e Projeto Básico.

b) Fiscal Técnico: Será indicado nominalmente pelo Diretor da SEGINFO, no despacho de aprovação dos Estudos Preliminares e Projeto Básico.

c) Fiscal Administrativo: Será indicado nominalmente pelo Diretor da Secretaria Administrativa e Financeira, por despacho ao determinar a abertura de procedimento administrativo.

4. Capítulo IV - ANÁLISE DE RISCOS

4.1. Riscos da Solução contratada não ter sucesso (riscos do produto/serviço)

RISCO 1	**Problema físico na Solução de Análise de Vulnerabilidades**
PROBABILIDADE	BAIXA
DANOS E IMPACTO	Em caso de parada da Solução, o impacto será baixo, pois todos os serviços, sistemas e endpoints do TRT12 continuarão disponíveis.

AÇÕES A SEREM TOMADAS PARA REDUZIR OU ELIMINAR OS RISCOS	**RESPONSÁVEL**
Manter os Data Centers refrigerados, com nobreaks funcionando corretamente e com os demais requisitos de ambiente verificados e corretos.	SEINFRA
DEFINIÇÃO DAS AÇÕES DE CONTINGÊNCIA A SEREM TOMADAS CASO OS RISCOS DE CONCRETIZEM	**RESPONSÁVEL**
Garantir que o backup da Solução de Análise de Vulnerabilidades esteja acessível e testado pela Secretaria de Tecnologia da Informação do TRT12.	Divisão de Segurança da Informação e Proteção de Dados

RISCO 2	**Falha no software de Análise de Vulnerabilidades.**
PROBABILIDADE	MÉDIA
DANOS E IMPACTO	Em caso de falha no software de Análise de Vulnerabilidades, o impacto será baixo, pois todos os serviços, sistemas e endpoints do TRT12 continuarão disponíveis.

AÇÕES A SEREM TOMADAS PARA REDUZIR OU ELIMINAR OS RISCOS	**RESPONSÁVEL**
Não atualizar o software de Análise de Vulnerabilidades pouco tempo antes do término do contrato de suporte.	Divisão de Segurança da Informação e Proteção de Dados
DEFINIÇÃO DAS AÇÕES DE CONTINGÊNCIA A SEREM TOMADAS CASO OS RISCOS DE CONCRETIZEM	**RESPONSÁVEL**
Capacitar a equipe de Infraestrutura para ter conhecimentos técnicos avançados, de forma que possam sanar eventuais falhas no software de Análise de Vulnerabilidades.	Divisão de Segurança da Informação e Proteção de Dados

5. Capítulo V - ASSINATURAS

Florianópolis, 14 de setembro de 2022

Equipe de Planejamento da Contratação

Integrante Demandante:

Nome: Valdir Luiz da Cunha
Cargo: Diretor da Secretaria da Tecnologia da Informação e Comunicação - SETIC
E-mail: valdir.cunha@trt12.jus.br

Integrante técnico:

Nome: Arthur Fernando Dellagiustina Lago
Cargo: Diretor da Divisão de Segurança da Informação e Proteção de Dados - SEGINFO
E-mail: arthur.lago@trt12.jus.br

Substituto:

Nome: Marcus Vinicius Mattos
Cargo: Técnico Judiciário
Email: marcus.mattos@trt12.jus.br

Integrantes administrativos:

Nome: Sérgio Moritz
Cargo: Analista Judiciário
E-mail: sergio.moritz@trt12.jus.br

Substitutos:

Nome: ARILDO DISARÓ FILHO
Cargo: Técnico Judiciário
Email: arildo.filho@trt12.jus.br