TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAZONAS
Av. André Araújo, S/N - Bairro Aleixo - CEP 69060-000 - Manaus - AM - www.tjam.jus.br

ESTUDO TÉCNICO PRELIMINAR - TJ/AM/SETIC/DVITIC

Responsáveis pela elaboração:
Washington Alves da Cunha Neto
Diogo Mendonça de Sousa

Contato: (92) 99118-9072
Número de identificação do ETP: 2454144
Categoria do Objeto: Serviços de Segurança da Informação.
CATSER: 27502

1. PLANO DE CONTRATAÇÕES ANUAL

1.1 O objeto da pretensa contratação, que consiste na aquisição de uma solução de análise de vulnerabilidade, desenvolvimento seguro e que contemple mecanismos antifraude, está previsto no Plano de Contratações Anual - PCA - do Poder Judiciário do Estado do Amazonas, sob o código **SETIC-2025-14**, conforme aprovado na **RESOLUÇÃO Nº 43, DE 22 DE OUTUBRO DE 2024** e disponibilizado no painel *BI* disponível NESTE LINK.

2. DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

2.1 O cenário atual da segurança da informação nas organizações públicas é marcado por ataques cibernéticos cada vez mais sofisticados e direcionados, exigindo que as instituições adotem soluções modernas, integradas e inteligentes para garantir a resiliência digital e a continuidade de seus serviços essenciais.

2.2 Embora o Tribunal de Justiça do Estado do Amazonas (TJAM) já disponha de soluções tradicionais de proteção, a crescente complexidade do ambiente, por possuir uma infraestrutura tecnológica de grande porte, composta por aproximadamente 500 servidores virtuais, inúmeros sistemas desenvolvidos internamente, mais de 60 comarcas e um contingente de mais de 4.500 usuários ativos entre magistrados, servidores e colaboradores, essa volumetria, aliada à criticidade dos serviços judiciais e administrativos, demanda um modelo de segurança que vai além de abordagens pontuais ou isoladas. Portanto, esse cenário impõe desafios significativos de controle, visibilidade e gestão de riscos cibernéticos, especialmente diante da crescente sofisticação dos ataques direcionados ao setor público.

2.3 A presente contratação visa à aquisição de uma solução integrada de análise, gestão de vulnerabilidades e ameaças, que consolide funcionalidades avançadas de apoio a detecção de ameaças, análises automatizadas de vulnerabilidades, proteção antifraude e práticas modernas de segurança no desenvolvimento de software (DevSecOps). A solução permitirá ao TJAM fortalecer significativamente sua postura de segurança cibernética, garantindo maior cobertura, automação, rastreabilidade e resposta frente a ameaças internas e externas. Essa abordagem contribui diretamente para uma gestão baseada em risco, alinhada à Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).

2.4 Para lidar com essa complexidade, a solução a ser contratada deve necessariamente prover uma visão centralizada e integrada de todo o ecossistema tecnológico do TJAM, permitindo a identificação automatizada de riscos, a gestão unificada das vulnerabilidades e exposições a ataques cibernéticos. Além disso, deve permitir que as equipes técnicas de segurança e desenvolvimento tenham acesso em tempo real a dashboards com indicadores de risco, criticidade, evolução de vulnerabilidades e ameaças em andamento, facilitando a tomada de decisão com base em dados concretos e atualizados.

2.4.1 A ausência dessa abordagem centralizada comprometeria diretamente a capacidade do TJAM de detectar e responder de forma eficiente a incidentes de segurança, resultando em maior tempo de exposição a ataques, ineficiência operacional, sobrecarga manual das equipes e aumento do risco institucional.

2.5 A contratação é absolutamente essencial para garantir a integridade, disponibilidade e confidencialidade dos ativos tecnológicos do Tribunal, com destaque para os seguintes aspectos:

2.5.1 Análise Contínua de Vulnerabilidades em Aplicações e Infraestrutura: A solução deve possibilitar de forma contínua a análise de segurança tanto em aplicações quanto nos componentes da infraestrutura tecnológica. Para isso, deverá contar com mecanismos capazes de realizar análises estáticas em artefatos de código, inspeção de bibliotecas e dependências externas, testes dinâmicos em aplicações em execução e avaliação de arquivos de definição de infraestrutura como código. Essa abordagem permitirá ao TJAM preservar a segurança de seus sistemas ao longo de todo o ciclo de vida, desde o desenvolvimento até a operação, conforme as boas práticas amplamente reconhecidas na área de segurança de aplicações.

2.5.2 Integração com Fluxos de Desenvolvimento Contínuo e Adoção de Práticas DevSecOps: A solução deverá ser compatível com plataformas de versionamento de código, ambientes de empacotamento de aplicações e fluxos automatizados de integração e entrega contínua, permitindo a inclusão de verificações de segurança de forma automatizada ao longo do ciclo de vida do desenvolvimento de software. Deverá conter recursos que bloqueiem a continuidade de versões identificadas como inseguras, contribuindo para o aumento da maturidade no desenvolvimento seguro da instituição. Essa capacidade viabiliza a aplicação prática de diretrizes DevSecOps, assegurando que vulnerabilidades sejam identificadas e tratadas antes da liberação dos sistemas em ambiente de produção.

2.5.3 Monitoramento de Vazamento de Credenciais e Exposição de Código: A solução deverá ser capaz de monitorar vazamentos de credenciais do TJAM na surface, deep e dark web, detectando inclusive informações publicadas em redes sociais, grupos de Telegram, GitHub, Pastebin, entre outros. Essa capacidade de inteligência cibernética contribui para a prevenção de incidentes de segurança e fraudes, fortalecendo os mecanismos de proteção à identidade institucional e à reputação do Tribunal.

2.5.4 Monitoramento e Proteção de Marca: A plataforma deve realizar o monitoramento automatizado de possíveis domínios fraudulentos e aplicativos móveis falsos, oferecendo análise preditiva de risco, captura de telas, e integração com bases públicas de registro de domínios. Além disso, detectar a utilização indevida de nomes do TJAM em redes sociais e marketplaces de aplicativos, funcionando como ferramenta antifraude essencial para a proteção da imagem institucional. Isso é especialmente relevante para o TJAM, dada sua visibilidade pública e o grande volume de interações com cidadãos, servidores e instituições parceiras.

2.6 A solução representará um salto qualitativo no modelo de defesa cibernética do TJAM, agregando inteligência, automação e visão preditiva à segurança institucional. Além de apoiar na mitigação de riscos operacionais, a solução promoverá ganhos operacionais, otimizará recursos e fortalecerá a transparência e a confiança social nos serviços prestados pelo Poder Judiciário.

2.7 Portanto, a realização de análises de vulnerabilidades no ambiente tecnológico do TJAM, são essenciais para identificação e correção de falhas em diferentes segmentos que podem ser exploradas por atacantes. O escopo destas análises precisa considerar desde o ambiente de produção até o ambiente de desenvolvimento de aplicações web, evidenciando possíveis problemas nos códigos-fonte que comprometam a segurança. Além disso, é necessário analisar a infraestrutura, verificando dispositivos, servidores e redes para encontrar vulnerabilidades e explorações (“exploits”) associadas que possam ser utilizadas por agentes maliciosos.

2.8 A contratação está em total conformidade com as diretrizes da Resolução CNJ nº 468/2022, que determina a adoção de medidas técnicas robustas para proteção de dados pessoais e segurança da informação; da Resolução CNJ nº 370/2021, que estabelece a necessidade de modernização da infraestrutura tecnológica e fortalecimento da resiliência cibernética no Poder Judiciário; e da Resolução CNJ nº 396/2021, que obriga a implementação de controles técnicos para a prevenção e resposta a incidentes de segurança. Além disso, a iniciativa está alinhada à Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), contribuindo diretamente para o fortalecimento da proteção de ativos críticos, a mitigação de ameaças cibernéticas e a elevação do nível de maturidade em segurança da informação no âmbito do TJAM.

3. UNIDADE DEMANDANTE

3.1 A unidade demandante responsável pelo desenvolvimento e acompanhamento deste estudo será a Secretaria de Tecnologia da Informação e Comunicação - SETIC.

4. REQUISITOS DA CONTRATAÇÃO

4.1. Trata-se da formação de Ata de Registro de Preços (ARP) para viabilizar a aquisição de uma solução integrada de gestão de vulnerabilidades e ameaças, contemplando funcionalidades de apoio a detecção de ameaças, análise de vulnerabilidades em aplicações e infraestrutura, monitoramento de exposições de credenciais e de domínios fraudulentos, com suporte a práticas modernas de desenvolvimento seguro (DevSecOps).

4.2 Sugere-se que a licitação seja realizada na Modalidade Pregão, na forma Eletrônica, tipo Menor Preço Global, mediante sistema de registro de preços.

4.3 Os eventuais acionamentos da ARP a ser formada resultarão em contratações de natureza contínua, uma vez que a ausência dessa solução poderia comprometer gravemente a integridade dos dados e a continuidade dos serviços judiciais e administrativos, diante do elevado número de servidores virtuais, sistemas e usuários.

4.4 A duração inicial da contratação será de 12 meses, podendo ser prorrogados sucessivamente, respeitada a vigência máxima decenal, conforme Art. 107 da Lei Federal n.° 14.133/2021.

4.5. A contratada deverá observar, sempre que aplicável, os critérios de sustentabilidade definidos no Guia Prático de Critérios de Sustentabilidade para Compras do TJAM, bem como os princípios da Política Nacional de Resíduos Sólidos, instituída pela Lei nº 12.305/2010.

4.6 O início da execução contratual deverá prever a transferência de conhecimento e tecnologia, promovendo uma relação mais transparente e colaborativa entre as partes. Essa transferência é essencial para:

4.6.1. Capacitar a equipe interna do TJAM a operar e manter a solução de forma autônoma;

4.6.2. Minimizar o tempo de resposta a incidentes;

4.6.3. Reduzir a dependência de suporte externo;

4.6.4. Manter a continuidade operacional com qualidade e segurança.

4.7. A contratada deverá fornecer treinamentos técnicos, documentação personalizada e suporte operacional para garantir a plena absorção dos conhecimentos relacionados a contratação pretendida.

4.8. A licitante deverá apresentar, na fase de habilitação, a seguinte documentação de qualificação técnica:

4.8.1. Comprovação de atividade econômica compatível com o objeto da contratação, por meio do CNAE correspondente.

4.8.2. Apresentação de, no mínimo, um atestado de capacidade técnica emitido por pessoa jurídica de direito público ou privado, que comprove experiência no fornecimento, implantação ou suporte da solução, demonstrando aptidão técnica na prestação de serviços relacionados à referida tecnologia;

4.8.3. Apresentação de certificação de competência e de revenda autorizada da solução;

4.9. No momento da assinatura do contrato, a licitante vencedora deverá comprovar que dispõe de no mínimo 01 profissional certificado na solução.

5. LEVANTAMENTO DE MERCADO E JUSTIFICATIVA DA ESCOLHA DO TIPO DE SOLUÇÃO A CONTRATAR

5.1. A presente contratação visa atender à necessidade de uma solução voltada à gestão de vulnerabilidades, proteção antifraude e desenvolvimento seguro (DevSecOps), a qual deve incluir, obrigatoriamente, funcionalidades de análise contínua de vulnerabilidades em aplicações e infraestrutura, apoio a resposta a incidentes de segurança, monitoramento de credenciais vazadas, códigos expostos e domínios fraudulentos, integração com esteiras de desenvolvimento. A solução deve abranger tanto a proteção do ambiente de Datacenter quanto os ciclos de desenvolvimento e operação de sistemas críticos do TJAM.

5.2 O TJAM já possui soluções tradicionais de segurança da informação em operação, como antivírus para estações de trabalho e servidores, firewall de próxima geração (NGFW), firewall de aplicação web (WAF) e solução PAM. No entanto, essas ferramentas, apesar de eficazes em seus domínios específicos, atuam de forma isolada e não são suficientes para enfrentar os desafios impostos pelas ameaças cibernéticas modernas.

5.3 As limitações dessas soluções tornam-se evidentes quando confrontadas com os seguintes requisitos estratégicos:

5.3.1 Análise contínua de vulnerabilidades (SAST, DAST, SCA, IaC): As soluções existentes não oferecem, de forma nativa, cobertura completa das técnicas de análise de vulnerabilidades em código-fonte, aplicações em execução, bibliotecas de terceiros e infraestrutura como código. A ausência dessa funcionalidade integrada demanda a aquisição e configuração de ferramentas especializadas adicionais, bem como esforço manual de integração.

5.3.2 Integração com esteiras CI/CD e DevSecOps: As ferramentas atuais não suportam, de maneira nativa, mecanismos de segurança embarcados nos pipelines de desenvolvimento. Falta a capacidade de bloquear automaticamente builds inseguros, realizar varreduras contínuas em containers e repositórios (como Git e Docker) e garantir a segurança de ponta a ponta no ciclo DevSecOps.

5.3.3 Monitoramento da Surface, Deep e Dark Web: Nenhuma das soluções em uso contempla recursos de proteção de marca voltados ao monitoramento externo de ambientes como Dark Web, Telegram, Pastebin e fóruns clandestinos, impossibilitando a detecção proativa de vazamentos de dados sensíveis e credenciais pertencentes ao TJAM.

5.3.4 Monitoramento e Proteção de Marca: Inexistem funcionalidades de proteção da marca institucional, como identificação de domínios maliciosos, aplicativos falsos ou tentativas de phishing direcionadas ao público externo. Esse tipo de monitoramento é fundamental para a preservação da imagem do TJAM.

5.3.5 Visão centralizada com dashboards de risco e correlação de eventos: Os painéis disponíveis nas soluções atuais são voltados à operação técnica e não fornecem uma visão estratégica. Falta uma interface única e integrada que consolide métricas de risco cibernético, indicadores de criticidade e impacto em tempo real, dificultando a tomada de decisões por parte da alta gestão.

5.4 Dessa forma, conclui-se que as soluções existentes no TJAM, apesar de robustas no que tange às suas respectivas funcionalidades, não atendem plenamente aos critérios técnicos e estratégicos exigidos pela presente contratação. Diante disso, justifica-se tecnicamente a adoção de uma solução especializada que reúna todas as capacidades mencionadas de forma integrada, automatizada e nativa, conforme exigências estabelecidas nos itens 2.1 a 2.8 deste ETP.

5.5 Portanto, optou-se por avaliar as alternativas de mercado com base em critérios técnicos de cobertura funcional, integração e arquitetura modular. Entre os principais fornecedores avaliados, destacaram-se: Checkmarx, Veracode, Rainforest, Qualys e Tenable.

Requisitos Funcionais	Checkmarx	Veracode	Rainforest	Qualys	Tenable
Gestão de Vulnerabilidades	Parcial	Parcial	Atende	Atende	Atende
Proteção Antifraude (Apps, Domínios, Sites)	Não atende	Não Atende	Atende	Atende	Não Atende
Desenvolvimento Seguro (DevSecOps)	Atende	Atende	Atende	Atende Parcial	Atende Parcial
Análise Contínua de Vulnerabilidades (Aplicações)	Atende	Atende	Atende	Atende	Atende Parcial
Análise Contínua de Vulnerabilidades (Infraestrutura)	Atende Parcial	Não Atende	Atende	Atende	Atende
Resposta Automatizada a Incidentes de Segurança	Atende Parcial	Atende Parcial	Atende	Atende	Atende
Threat Inteligence	Não Atende	Não Atende	Atende	Atende Parcial	Atende Parcial
Monitoramento de Credenciais Expostas	Não Atende	Não Atende	Atende	Atende Parcial	Atende Parcial
Integração com Esteiras de Desenvolvimento (DevOps)	Atende	Atende	Atende	Atende Parcial	Atende Parcial

5.5.1 Checkmarx: Forte no desenvolvimento seguro e análise de vulnerabilidades em aplicações.

5.5.1.1 Atua com SAST, DAST, SCA, IaC e possui boa integração DevSecOps.

5.5.1.2 Parcial em gestão de vulnerabilidades, pois cobre apenas segurança de código, não infraestrutura ou ativos externos.

5.5.1.3 Não possui módulos antifraude ou monitoramento de vazamentos.

5.51.4 Resposta automatizada é limitada a correção de código, sem integração com SIEM ou fluxos de takedown.

5.5.2 Veracode: Muito bom em segurança de aplicações e pipelines DevSecOps:

5.5.2.1 SaaS com baixa taxa de falso-positivo, integrações com IDEs e CI/CD.

5.5.2.2 Parcial em gestão de vulnerabilidades, pois cobre aplicações, mas não infraestrutura;

5.5.2.3 Não possui recursos para antifraude ou monitoramento externo.

5.5.2.4 Resposta automatizada se limita à sugestão de correção (AI Fix), sem automação e apoio de resposta a incidentes em infraestrutura.

5.5.3 Rainforest: Atende todos os critérios, oferecendo módulos específicos para Aplicação, Infraestrutura, Fraude e Vazamentos, se integra facilmente com esteiras DevOps. Sua plataforma provê inteligência acionável para resposta a incidentes, incluindo takedowns.

5.5.4 Qualys: Amplo em infraestrutura e vulnerabilidades externas.

5.5.4.1 Inclui VMDR, Web Application Scanning, e Asset Management com proteção antifraude e descoberta de domínios externos (ASM/EASM).

5.5.4.2 Boa resposta automatizada com integração a ITSM.

5.5.4.3 Parcial em DevSecOps, pois sua integração com pipelines não é nativa e exige configuração adicional.

5.5.4.4 Falta suporte nativo ao leak monitoring de credenciais, antifraude em apps ou segurança de código.

5.5.5 Tenable: Especialista em segurança de infraestrutura, cloud e OT.

5.5.5.1 Integração com DevOps, CI/CD, IaC scanning e dashboards de risco.

5.5.5.2 Parcial em aplicação: cobre apps web, mas não no nível de soluções como Veracode ou Checkmarx.

5.5.5.3 Não possui módulo dedicado a antifraude nem a monitoramento de domínios maliciosos.

5.5.5.4 Parcial no monitoramento de vazamentos, pois foca em exposição de ativos internos.

5.6 A análise comparativa objetivava identificar, com imparcialidade técnica, os pontos fortes e limitações de cada solução, possibilitando uma escolha fundamentada e estratégica. Foram avaliados aspectos como: Integração nativa das funcionalidades, cobrindo (DevSecOps, antifraude, gestão de vulnerabilidades), interoperabilidade, escalabilidade, custo estimado, riscos associados e aderência às necessidades institucionais.

5.8 Portanto, a solução Rainforest se destacou como a solução mais completa e integrada, por cobrir todos os critérios com módulos nativos.

6. DESCRIÇÃO DA SOLUÇÃO ESCOLHIDA

6.1. A descrição da solução como um todo deverá atender aos seguintes itens:

Item	Descrição
1	Detecção e Mitigação de Vulnerabilidades em Aplicações para 12 meses
2	Detecção e Mitigação de Vulnerabilidades em Infraestrutura para 12 meses
3	Análise de Exposição de Dados e Credenciais para 12 meses
4	Detecção de Domínios Fraudulentos para 12 meses
5	Módulo de treinamentos para os itens 01, 02, 03 e 04

6.2. ITEM 01 - Detecção e Mitigação de Vulnerabilidades em Aplicações

6.2.1 A solução deve permitir análise de até 10 aplicações em desenvolvimento e/ou já existentes no ambiente de produção do TJAM.
6.2.2 Toda a análise de códigos fonte deverá ocorrer dentro do perímetro de segurança do TJAM e/ou fábrica de software onde a aplicação esteja sendo desenvolvida, de acordo com as políticas de segurança definidas pelo TJAM, visando a proteção de Propriedade Intelectual.
6.2.3 Para fins de análise do código-fonte, não deverá ser realizado envio (upload) para a nuvem da CONTRATADA ou de terceiros.
6.2.4 Deve ser compatível com protocolo Git com o objetivo de se conectar no repositório de código-fonte do TJAM.
6.2.5 A solução deverá ser apta e ter opção de contexto, e permitir que a CONTRATADA clique e armazene pequenos trechos de código-fonte a fim de permitir ao desenvolvedor que identifique rapidamente o contexto em que a vulnerabilidade foi detectada.
6.2.6 A solução deve permitir a integração direta (plug and play) com repositório de código-fonte (Git) e repositório de imagens (Docker) interdependente da esteira DevOps de desenvolvimento (Jenkins, Gitlab, Azure DevOps ou qualquer outra existente que se utilize o protocolo Git), permitindo acesso às funcionalidades de análise de vulnerabilidades sem depender da esteira CI/CD.
6.2.7 A solução deve permitir, quando necessário, bloqueio de esteira para que a aplicação não siga em frente para produção (funcionalidade conhecida como gatekeeper), no mínimo nos seguintes cenários:
6.2.7.1 Bloquear a esteira caso seja detectado que a aplicação ou imagem foi gerada a partir de um código que não atendeu as etapas obrigatórias do processo de análise de segurança, garantindo a conformidade com as políticas de governança estabelecidas.
6.2.7.2 Quando houver alguma vulnerabilidade considerada alta ou crítica não tratada.
6.2.7.3 Quando houver código sensível identificado na análise de código-fonte com objetivo de detectar e alertar sobre melhorias de qualidade de código.
6.2.8 A solução deve possuir funcionalidade para análise de código e detectar e alertar sobre vulnerabilidades de segurança (SAST – Static Application Security Testing).
6.2.9 A solução deve possuir funcionalidade para análise de segurança de terceiros (SCA – Software Composition Analysis).
6.2.10 A solução deve possuir funcionalidade para varredura de vulnerabilidades dinâmicas na aplicação (DAST – Dynamic Application Security Testing).
6.2.11 A solução deve possuir funcionalidade para varredura em containers, Docker, para detectar vulnerabilidades de segurança.
6.2.12 A solução deve possuir funcionalidade para análise de vulnerabilidades em aplicações móveis (MAST – Mobile Application Security Testing).
6.2.13 A solução deve possuir funcionalidade para análise de segurança em infraestrutura como código (IaC – Infrastructure as Code), por exemplo, Ansible e Terraform.
6.2.14 A solução deve ter capacidade de identificação de vulnerabilidades do OWASP TOP10.
6.2.15 A solução deve possuir funcionalidades para análise de código com recomendações de melhoria de qualidade.
6.2.16 A solução deverá fornecer recomendações para correções (utilizando a base de conhecimentos da própria plataforma ou implementando funcionalidades de inteligência artificial para apresentar tais recomendações).
6.2.17 A solução deve gerar alertas de vulnerabilidades via plataforma: e-mail, Telegram e/ou Slack.
6.2.18 A solução deve possuir painel (dashboard) que apresente o nível de risco de código-fonte e infraestrutura por criticidade.
6.2.19 Deve apresentar painel (dashboard) do ciclo DevSecOps com painel de vulnerabilidades por etapa, com no mínimo as etapas “Quality”, “SAST”, “SCA”, “DAST”, “Image”, “MAST” e “IaC”.
6.2.20 A solução deve possuir funcionalidade para classificar as vulnerabilidades como falso-positivo, a priorizar ou mitigado em outro ambiente.
6.2.21 A solução deve permitir análise contínua, bastante a atualização do código pelo desenvolvedor, para que a plataforma inicie a análise de código.
6.2.22 A solução deve permitir o cadastro manual de vulnerabilidades.
6.2.23 A solução deve disponibilizar uma extensão (plugin) que permita acompanhar os achados de vulnerabilidade em ambiente de desenvolvimento integrado (Integrated Development Environment – IDE) suportando soluções como Microsoft Visual Studio Code.

6.3. ITEM 02 Detecção e Mitigação de Vulnerabilidades em Infraestrutura

6.3.1 A Solução deve analisar até 500 dispositivos da infraestrutura do TJAM a serem definidos pela SETIC.
6.3.2 Deve possibilitar o cadastro manual de redes e ativos de redes individuais, com cadastro do endereço IP, departamento, localização geográfica, nome e descrição do ativo.
6.3.3 Deve conter um cadastro manual de tecnologias instaladas em um ativo no inventário, com no mínimo informações como: fabricante, produto e versão.
6.3.4 Deve contar com funcionalidade própria de inventário automatizado dos ativos do ambiente, com suporte a inventário usando credenciais de acesso aos ativos.
6.3.5 Deve ser capaz de identificar ativos existentes em uma faixa (range) de rede e cadastrá-los na plataforma aos poucos.

6.3.6 Deve ser capaz de autenticar nos ativos encontrados e realizar o inventário automatizado de todas as tecnologias instaladas em cada um dos equipamentos servidores e estações de trabalho do escopo.
6.3.7 Deve reconhecer e inventariar tecnologias, como Java, Bancos de dados (SQL Server, MySQL, MariaDB, Oracle), Sistemas operacionais (Windows, Linux, MacOS, IOS, Android), Ferramentas de usuários (Pacotes Office, VSCode, Adobe Acrobat e Acrobat Reader).
6.3.8 Deve ser capaz de realizar varreduras de vulnerabilidades dos ativos identificados através do inventário, em períodos definidos no próprio sistema.
6.3.9 Deve possuir opção para iniciar varredura de vulnerabilidades via agendamento.
6.3.10 Deve permitir que sejam definidos janelas para execução das varreduras com o objetivo de limitar a data e horário de início e final das análises que serão realizadas no ativo.
6.3.11 Todas as vulnerabilidades detectadas pela análise de vulnerabilidades devem ser armazenadas pela plataforma para gestão.
6.3.12 Armazenar, também, todas as vulnerabilidades vinculadas a uma determinada tecnologia já lida.
6.3.13 Deve ser capaz de identificar novas vulnerabilidades nos ativos inventariados, sem execução de varreduras e sem geração de tráfego baseando-se nas tecnologias do ativo.
6.3.14 A solução deve gerar alertas de vulnerabilidades via plataforma: e-mail, Telegram e/ou Slack.
6.3.15 Deve contar com opções de notificação, para que o gestor possa selecionar quais as suas preferências para recebimento de alertas.
6.3.16 Deve ser capaz de integrar com ferramentas de Endpoint Detection and Response (EDR).
6.3.17 Deve permitir a configuração do período, em dias, que um dispositivo será automaticamente descomissionado se permanecer inativo (sem análise de vulnerabilidade ou descoberta), ou seja, removido do inventário de dispositivos da plataforma a fim de sanitizá-la.
6.3.18 Deve permitir que este seja a quantidade de dias seja configurada especificamente por técnica de descoberta do ativo, por exemplo, aqueles que foram identificados por análise de vulnerabilidade (X dias) ou através da integração com EDR (Y dias).
6.3.19 Possibilitar a configuração de janelas (períodos) onde a análise de infraestrutura poderá ser executada. Caso a análise de vulnerabilidade ultrapasse a janela configurada, a plataforma deverá pausar a análise e retomá-la assim que possível (próxima janela de execução).

6.4. ITEM 03 – Análise de Exposição Dados e Credenciais

6.4.1 A Solução deve detectar vazamentos de informações sensíveis do TJAM com base em definições de um domínio e até 05 palavras-chave a serem definidas pelo TJAM;
6.4.2 Detectar vazamento de credenciais com base nos domínios e palavras-chave a serem definidas em conjunto pelo TJAM e CONTRATADA.
6.4.3 Deve realizar busca em múltiplas fontes que monitorem surface, deep e/ou dark web.
6.4.4 Deve realizar a classificação das credenciais que foram descobertas, incluindo aquelas que são diretamente de servidores do TJAM, mas também aquelas que são de clientes/usuários do TRIBUNAL, ou seja, usuários que utilizam serviços do TJAM.
6.4.5 Deve implementar formas automatizadas para a classificação dos itens que foram identificados reduzindo, sempre que possível, o esforço da análise / categorização manual.
6.4.6 Deve permitir, de forma macro, visualizar e correlacionar as credenciais das listas de registros encontradas a fim de evitar que os mesmos registros que foram identificados sejam expostos.
6.4.7 Deve implementar monitoramento de grupos de Telegram, onde são divulgadas informações dessa natureza.
6.4.8 As credenciais identificadas devem sempre que possível conter as seguintes informações: Classificação do vazamento, usuário (e-mail vazado), senha (password), alvo do acesso (site, URL, etc), descrição, data de vazamento e data da descoberta do vazamento.

6.4.9 Detectar vazamento de códigos-fonte de aplicações de desenvolvimento interno, com base em palavras-chave a serem definidas em conjunto pelo TJAM e CONTRATADA.
6.4.10 Deve verificar repositórios de códigos-fonte públicos como, por exemplo, GitHub, Gitlab, Postman e endereços de armazenamento de texto como, por exemplo, o site Pastebin com o objetivo de detectar compartilhamento indevido de informações corporativas.
6.4.11 Detectar referências (links) para os domínios e/ou palavras-chave que sinalizem uma possibilidade de vazamentos de documentos ou serviços do TJAM.

6.4.12 A solução deve possuir painéis que apresentem de forma consolidada um resumo do status atual da análise com base em classificações, indicando a evolução da análise dos achados, ou seja, quantos estão em análise e quantos foram fechados ou resolvidos.
6.4.13 Para as funcionalidades de monitoramento de fraude e vazamento de informação que permitam a classificação das informações identificadas pelo sistema, deve possibilitar a classificação de um item identificado, pelo menos, como:
6.4.13.1 sob análise, para itens que foram encontrados e precisam ser verificados;
6.4.13.2 confiável ou resolvido, para itens que foram encontrados, mas são confiáveis ou já foram resolvidos;
6.4.13.3 irrelevante, para itens que foram encontrados e não representam risco ou fraude.
6.4.14 Possibilidade de personalizar quais colunas serão exibidas e em qual ordem serão exibidas.
6.4.15 Possibilidade de exportar as informações da tabela que são apresentadas na tela para valores separados por vírgulas ou ponto e vírgula (CSV – comma separated values).

6.5. ITEM 04 – Detecção de Domínios Fraudulentos

6.5.1 A Solução deverá realizar as análises de Fraudes Web com base em definições de um domínio e até 05 palavras-chave a serem definidas pelo TJAM;
6.5.2 Deve realizar monitoramento de nomes de domínio cadastrados na Internet, para identificar nomes semelhantes aos domínios monitorados (tipo de ataque também conhecido como cybersquatting).
6.5.3 Deve detectar possíveis domínios fraudulentos e permitir a notificação através da própria plataforma, e-mail, Telegram e/ou Slack.
6.5.4 Deve, sempre que possível, fornecer uma foto (screenshot) da tela (homepage) do possível domínio fraudulento.
6.5.5 Deve, sempre que possível, fornecer informações de cadastro do domínio (whois).
6.5.6 Utilizar de múltiplas inteligências (por exemplo: algoritmos de registro) para descoberta de possíveis domínios fraudulentos.
6.5.7 Consultar, no ato do registro, a legitimidade do domínio.
6.5.8 Apresentar uma pontuação (score) indicando a probabilidade de o IP para qual o domínio aponta ser utilizado para fraude, com o objetivo de possibilitar a priorização de ações.
6.5.9 Deve apresentar se o site em questão tiver selo seguro (HTTPS), qual a data de expiração do certificado SSL.
6.5.10 A funcionalidade de proteção de aplicações móveis deve ser capaz de permitir o cadastro de palavras-chave e nomes de aplicativos móveis (apps) que o TJAM tenha atualmente ou venha a ter para monitoramento.
6.5.11 Deve monitorar lojas de aplicativos (marketplaces) oficiais e não-oficiais, como Google Play, Apple Store e Aptoide, para detectar aplicativos que possam utilizar o nome do TJAM com objetivo de realizar fraudes.
6.5.12 Deve detectar possíveis aplicativos móveis falsos com o nome do TJAM, através da plataforma: e-mail, Telegram e/ou Slack.
6.5.13 A plataforma deverá executar o monitoramento periódico de tais informações de forma automatizada.
6.5.14 A funcionalidade de redes sociais (social networks) deve possibilitar o monitoramento de redes sociais com objetivo de identificar usuários, páginas e postagens (posts) que façam referência às palavras-chave que são monitoradas.
6.5.15 A solução deve realizar buscas, no mínimo nas seguintes redes sociais: Facebook, Instagram, TikTok, X (Twitter) e YouTube, trazendo informações que estejam disponíveis como “likes”, “comments”, “shares”, “posts”, “followers”, “following”.
6.5.16 Possibilidade de adicionar o usuário na lista de usuários permitidos (“add user to whitelist”) com o objetivo que todas as publicações do usuário já sejam automaticamente classificadas como permitidas (whitelisted).
6.5.17 A plataforma deverá executar o monitoramento periódico de redes sociais de forma automatizada.
6.5.18 A funcionalidade de web de superfície ou conteúdo indexado (surface web) deve possibilitar o monitoramento de conteúdos que estejam indexados em buscadores como, por exemplo, Google, repositórios de objetos ou arquivos (buckets AWS S3, por exemplo) e blogs.
6.5.19 Tal funcionalidade tem como objetivo identificar itens que não em categorias referenciadas anteriormente, contudo mesmo assim representem potencial risco de fraude ao TJAM.
6.5.20 Deve possibilitar a criação de marcação ou posicionamento específico, no momento da análise de páginas de fraudes que copie o conteúdo do TJAM ou conduta de redirecionamento da página e/ou que fazem referência a ela.
6.5.21 Tal funcionalidade tem como objetivo reduzir o tempo de identificação de páginas falsas que são utilizadas pelos fraudadores.
6.5.22 A solução deve possuir dashboards que apresentem de forma consolidada um resumo do status atual da análise dos achados, ou seja, quantos estão em análise e quantos foram fechados ou resolvidos.

6.5.23 Para as funcionalidades de monitoramento de fraude e vazamento de informação que permitam a classificação das informações identificadas pelo sistema, deve possibilitar a classificação de um item identificado, pelo menos, como:
6.5.23.1 sob análise (under analysis), para itens que foram encontrados e precisam ser verificados;
6.5.23.2 confiável (trusted) ou resolvido (solved), para itens que foram encontrados, mas são confiáveis ou já foram resolvidos;
6.5.23.3 irrelevante (irrelevant), para itens que foram encontrados e não representam risco ou fraude.
6.5.24 Possibilidade de personalizar quais colunas serão exibidas e em qual ordem serão exibidas.
6.5.25 Possibilidade de exportar as informações da tabela que são apresentadas na tela para valores separados por vírgulas ou ponto e vírgula (CSV – comma separated values).

6.6. Especificação técnica comum aos itens 01, 02, 03 e 04

6.6.1 Contratação de solução de segurança no modelo híbrido (parte SaaS (Software as a Service) e parte on-premise capaz de realizar análise, monitoramento e acompanhamento de parâmetros de segurança no processo de gestão de vulnerabilidade desde o desenvolvimento de software até a proteção da marca (reputação) do TJAM.
6.6.2 A solução contratada deverá atender, diretamente ou em composição, aos seguintes requisitos desta contratação:
6.6.2.1 No caso de composição de soluções e necessidade de integração, a CONTRATADA fornecerá ao TJAM um painel único, seguro, com uma única autenticação que mostre as informações de vulnerabilidades e proteção de reputação centralizadas.
6.6.2.2 A solução deverá mostrar e possibilitar a integração de funcionalidades de vulnerabilidade incluindo infraestrutura, desenvolvimento seguro (DevSecOps) e proteção de reputação.
6.6.3 A solução deve contar com uma interface web intuitiva para acesso às funcionalidades.
6.6.3.1 A plataforma deverá atender os módulos dos itens 01, 02, 03 e 04.
6.6.4 Implementar controle de acesso baseado em permissões de usuários para as funcionalidades da solução.
6.6.5 Deverá conter, pelo menos, três papéis (funções) de usuário pré-definidas: administrador, operador e visualizador. Cada nível restringirá as configurações e ações que o usuário poderá realizar em cada um dos módulos da solução.
6.6.6 Possibilidade de configurar um segundo fator de autenticação (2FA) com base em códigos baseados em chaves digitais (soft tokens) através de aplicativos como: Microsoft Authenticator e Google Authenticator.
6.6.7 Possibilidade de configurar o segundo fator de autenticação (2FA) como obrigatório para todos os usuários que utilizam a plataforma; ou
6.6.7.1 Possibilidade de configurar o segundo fator de autenticação como não obrigatório, podendo individual ape-nas para alguns usuários que utilizam a plataforma.
6.6.8 Possibilidade de configurar Single Sign On (SSO) para autenticação através de identidade federada com, no mínimo, as seguintes soluções:
6.6.8.1 Microsoft Active Directory Federation Services (ADFS)
6.6.8.2 Okta
6.6.9 Possibilidade de escolher o idioma de interface suportando, no mínimo, 2 idiomas: português e inglês.
6.6.9.1 Deve permitir que o usuário selecione um idioma padrão que já esteja salvo toda vez que ele abrir a solução.
6.6.10 Deve possuir uma área de consulta (referência rápida) onde o usuário realizará uma busca que inclua, no mínimo, as seguintes informações:
6.6.10.1 Sobre CVE (Common Vulnerabilities and Exposures): apresentar informações gerais sobre a vulnerabilidade como, por exemplo, pontuação (score), vetor de ataque (attack vector), referências externas, deverá manter-se atualizada sobre tendências, dispositivos e aplicações que são afetadas, além de exploits que já estejam disponíveis para explorar tal vulnerabilidade.
6.6.10.2 Sobre TTP (Tactics, Techniques and Procedures): referência geral à estrutura (framework) do MITRE ATT&CK sobre técnicas, táticas e procedimentos de atacantes para facilitar a consulta na solução sem que seja necessário visitar site externo.
6.6.11 Deve disponibilizar API (Application Programming Interface) para permitir integração com outras soluções do ambiente do TJAM podendo consumir os dados gerados pela plataforma.
6.6.12 Deve permitir a realização de ações em lote para a classificação dos achados da plataforma, possibilitando:
6.6.12.1 Seleção de múltiplos itens para classificação.
6.6.12.2 Seleção de múltiplos itens para edição de severidade, que se estenda para um ação possível da plataforma.
6.6.12.3 Incluir comentários em achados, sempre que possível.
6.6.12.4 Seleção de múltiplos itens para ações, sempre que se tratar de uma ação possível da plataforma.
6.6.13 Deve possibilitar a adição e visualização de comentários de atividade nos achados para que seja possível rastreabilidade e trabalho colaborativo entre os usuários da plataforma.

6.7. Especificação técnica comum aos itens 01 e 02.

6.7.1 A solução deve implementar tecnologia para análise dos códigos-fonte, através de concentradores de análise que deverão ser instalados dentro da infraestrutura (on-premises ou cloud) do TJAM de forma centralizada utilizando recursos de máquinas virtuais do próprio TJAM.
6.7.2 Entende-se por forma centralizada, não ser necessária a instalação em cada equipamento do desenvolvedor e/ou servidor de repositório de código-fonte.
6.7.3 Os concentradores de análise deverão ser compatíveis, no mínimo, com as seguintes versões de Sistema Operacional:
6.7.3.1 Ubuntu 18.04.6 LTS (Bionic), 20.04.2 LTS (Focal) e 22.04.5 (Jammy Jellyfish).
6.7.4 Todas as credenciais que forem cadastradas na plataforma para acesso aos serviços do TJAM deverão ser armazenadas de forma segura garantindo que, uma vez cadastradas pelo TJAM, não sejam exibidas novamente na interface web em texto claro.
6.7.5 Todo tráfego de informação como credenciais, descobertas de vulnerabilidades ou outros tipos de comunicação entre a plataforma e os concentradores de análise deverá ser realizado através de protocolo seguro usando criptografia.
6.7.6 Sempre que houver uma nova varredura de vulnerabilidades, deverá ser atualizada a lista de vulnerabilidades ativas aquelas que não forem mais detectadas, mantendo assim as informações atualizadas.
6.7.7 Permitir a classificação dos itens de vulnerabilidade como redes, ativos, aplicações, etc através do uso de marcações conhecidas como tags ou labels a fim de organizar e agrupá-los, devendo permitir a criação e customização de novas marcações.
6.7.8 Para cada conjunto de análise que a plataforma executar, deverá fornecer painel (dashboard) com visão geral do cenário atual de vulnerabilidades, bem como sua evolução e priorização. Tal painel deverá apresentar, no mínimo, as seguintes informações:
6.7.8.1 Achados por categoria (possibilitando filtrar: baixas, médias, altas e críticas).
6.7.8.2 Total de dispositivos ou achados.
6.7.8.3 Total de vulnerabilidades.
6.7.8.4 Classificação dos achados por família.
6.7.8.5 Priorização com base na criticidade da vulnerabilidade, na probabilidade (likelihood) e ativos do ambiente do TJAM através de um gráfico que agrupe: urgente (corrigir agora), alta (corrigir depois), média (planeje corrigir) e baixa (corrigir depois de todas as outras).
6.7.8.6 Vulnerabilidades ou achados novos ou resolvidos por período.
6.7.8.7 Evolução dos achados ao longo do tempo.
6.7.8.8 Lista configurável com, por exemplo, os 10, 15, 20, 50 ou 100 ativos com mais vulnerabilidades no ambiente.
6.7.9 Para cada conjunto de análise que a plataforma executar, deverá fornecer uma visualização em lista de itens que ao clicar permite entender quais vulnerabilidades estão associadas com aquele dispositivo ou aplicação.
6.7.10 Tais vulnerabilidades ou achados deverão ser agrupados, no mínimo, pelos seguintes critérios: abertos, mitigados, transferidos, fechados, não aplicáveis ao ambiente do TJAM (falso-positivos) ou removidos por automação da plataforma (descomissionados).
6.7.11 Deve permitir filtrar as informações das vulnerabilidades com base nas seguintes informações:
6.7.11.1 Severidade (crítica, alta, média e baixa).
6.7.11.2 Família.
6.7.11.3 Tecnologia.
6.7.11.4 Status do achado (aberto, mitigado, transferido, fechado, falso-positivo e descomissionados).
6.7.11.5 Nome do achado/vulnerabilidade.
6.7.11.6 CVSS (pontuação da família ou conformidade).
6.7.11.7 Marcações (Tags ou Labels).
6.7.11.8 Datas: item criado, item em reanálise e/ou reintervenção e/ou intervenção e data que foi fechado.

6.7.12 Deve possibilitar a exportação das informações apresentadas na plataforma (com base nos filtros aplicados) para valores separados por vírgulas ou ponto e vírgula (CSV – comma separated values).

6.8. ITEM 05 – Módulo de Treinamento nos Itens 01, 02, 03 e 04

6.8.1. Será necessário treinamento à equipe que atuará com a solução. O TJAM irá definir a qual item deste objeto o módulo de treinamento irá abranger
6.8.2. O módulo de treinamento deverá ser de no mínimo 8 horas de duração, podendo ser dividi-do em 4 horas diárias.
6.8.3. Poderá ser realizado de forma presencial, na estrutura do TJAM, ou remoto, a ser definido pelo TJAM.
6.8.4. Deverá possuir uma turma de até 10 participantes, a serem definidos pelo TJAM
6.8.5. O conteúdo do módulo de treinamento deverá abranger toda a solução fornecida no item a ser definido pelo TJAM, esclarecendo a arquitetura e configurações executadas
6.8.6. Os instrutores deverão possuir experiência e certificação na área de segurança da informação

7. DA NECESSIDADE DE FORMALIZAÇÃO DE CONTRATO

7.1 Os eventuais acionamentos da Ata de Registro de Preço (ARP) resultante do pregão ensejarão formalização de contrato para os serviços previstos neste Estudo Técnico Preliminar (ETP), tendo em vista as características do objeto a ser contratado, com a existência de obrigações futuras, incluindo a garantia, continuidade e confiabilidade do mesmo.

7.2 O contrato oriundo de eventual acionado da ARP terá duração de 12 (doze) meses, podendo ser prorrogados sucessivamente, respeitada a vigência máxima decenal, conforme Art. 107 da Lei Federal n.° 14.133/2021.

8. ESTIMATIVAS DAS QUANTIDADES PARA A CONTRATAÇÃO

8.1. Tendo por objetivo assegurar a proteção contínua das aplicações críticas do Tribunal de Justiça do Estado do Amazonas (TJAM), garantir a alta disponibilidade dos serviços judiciais e administrativos, fortalecer a segurança cibernética e atender às exigências normativas vigentes, estima-se contratar:

GRUPO	ITEM	ESPECIFICAÇÕES	QUANTIDADE MÍNIMA POR CONTRATAÇÃO	QUANTIDADE TOTAL
01	**Detecção e Mitigação de Vulnerabilidades em Aplicações para 12 meses**			
	1	Licença base para habilitar os recursos de vulnerabilidade de aplicações.	01	01
	2	10 aplicações para todos os recursos que utilizam aplicação.	01	04
02	**Detecção e Mitigação de Vulnerabilidades em Infraestrutura para 12 meses**			
	3	Licença base para habilitar os recursos de ativos e vulnerabilidades de ameaças.	01	01
	4	100 ativos para todos os recursos que utilizam ativo.	01	06
03	**Análise de Exposição de Credenciais para 12 meses**			
	5	Licença base para habilitar os recursos de detecção de vazamento.	01	01
04	**Detecção de Domínios Fraudulentos para 12 meses**			
	6	1 domínio para todos os recursos que utilizam domínio.	01	04
	7	Licença base para habilitar os recursos de detecção de fraude.	01	01
	8	5 palavras-chave para todos os recursos que utilizam palavra-chave.	01	04
05	**Módulo de treinamentos**			
	9	Módulo de treinamento para os grupos 01, 02, 03 e 04	01	01

9. ESTIMATIVAS DAS QUANTIDADES PARA A CONTRATAÇÃO

9.1 Os valores estimados para esta contratação seguem na planilha abaixo.

GRUPO	ITEM	ESPECIFICAÇÕES	QUANTIDADE MÍNIMA POR CONTRATAÇÃO	QUANTIDADE TOTAL	UND	PREÇO (R$)	PREÇO TOTAL (R$)
01	**Detecção e Mitigação de Vulnerabilidades em Aplicações para 12 meses**						
	1	Licença base para habilitar os recursos de vulnerabilidade de aplicações.	01	01	Unidade	R$ 47.560,13	R$ 47.560,13
	2	10 aplicações para todos os recursos que utilizam aplicação.	01	04	Unidade	R$ 195.135.97	R$ 780.543.88
02	**Detecção e Mitigação de Vulnerabilidades em Infraestrutura para 12 meses**						
	3	Licença base para habilitar os recursos de ativos e vulnerabilidades de ameaças.	01	01	Unidade	R$ 10.870,89	R$ 10.870,89
	4	100 ativos para todos os recursos que utilizam ativo.	01	06	Unidade	R$ 15.207,86	R$ 91.247,19
03	**Análise de Exposição de Credenciais para 12 meses**						
	5	Licença base para habilitar os recursos de detecção de vazamento.	01	01	Unidade	R$ 40.765,53	R$ 40.765,53
	Detecção de Domínios Fraudulentos para 12 meses						
04	6	1 domínio para todos os recursos que utilizam domínio.	01	04	Unidade	R$ 7.473,74	R$ 29.894,94
	7	Licença base para habilitar os recursos de detecção de fraude.	01	01	Unidade	R$ 54.354,44	R$ 54.354,44
	8	5 palavras-chave para todos os recursos que utilizam palavra-chave.	01	04	Unidade	R$ 6.414,97	R$ 25.659,87
	Módulo de treinamentos						
05	9	Módulo de treinamento para os grupos 01, 02, 03 e 04	01	01	Unidade	R$ 80.000,00	R$ 80.000,00
VALOR TOTAL ESTIMADO DO SRP							**R$ 1.160.896,87**

10. JUSTIFICATIVA PARA PARCELAMENTO OU NÃO DA CONTRATAÇÃO

10.1 Por se tratar de uma contratação em que os itens possuem a mesma natureza técnica, sendo portanto interdependentes entre si, entendemos que o parcelamento da solução não se mostra viável. Portanto, todos os itens deverão ser entregues e implantados por uma única empresa, de modo a evitar fornecimento incompleto e/ou compartilhamento e confusão de responsabilidades entre diferentes fornecedores.

11. CONTRATAÇÕES CORRELATAS/INTERDEPENDENTES

11.1 Não há contratações correlatas.

12. RESULTADOS PRETENDIDOS

12.1 Fortalecimento da Postura de Segurança Cibernética: o TJAM passará a contar com um nível elevado de maturidade em segurança da informação, sustentado por uma solução integrada que permitirá a análise contínua de vulnerabilidades em aplicações, infraestrutura e ambientes de desenvolvimento, proporcionando visão centralizada e resposta proativa a incidentes.

12.2 Integração com Práticas DevSecOps: os pipelines de desenvolvimento (CI/CD) estarão plenamente integrados a controles automatizados de segurança, permitindo que vulnerabilidades sejam identificadas e tratadas antes da publicação de novos sistemas ou atualizações, reduzindo significativamente o risco de exposição a ataques cibernéticos.

12.3 Mitigação de Riscos de Vazamento de Dados e Fraudes Digitais: o Tribunal contará com mecanismos permanentes de monitoramento de credenciais, detecção de domínios fraudulentos e proteção de marca em ambientes como surface, deep e dark web, prevenindo fraudes, clonagem de domínios e uso indevido da identidade institucional.

12.4 Automação na Gestão de Vulnerabilidades: a gestão de vulnerabilidades será marcada por alta automação, permitindo a priorização de riscos, a classificação de vulnerabilidades e a geração de recomendações de correção com maior agilidade e eficiência das equipes técnicas.

15. SERVIÇOS DE MANUTENÇÃO E ASSISTÊNCIA TÉCNICA

15.1. Durante toda a vigência contratual, a Contratada deverá assegurar a disponibilização contínua de atualizações corretivas, evolutivas e de segurança para todos os componentes licenciados, abrangendo também, quando aplicável, os elementos instalados no ambiente on-premise, de modo a garantir que a solução permaneça permanentemente atualizada, protegida contra novas vulnerabilidades e em plena conformidade com as recomendações técnicas e melhores práticas do fabricante.

15.2 Por ser uma solução baseada predominantemente em nuvem, as manutenções serão realizadas na sede da empresa fornecedora dos serviços ou na própria fabricante.

15.3 As paradas técnicas para manutenção deverão ser avisadas com antecedência mínima de 3 (três) dias úteis.

16. DECLARAÇÃO DE VIABILIDADE (OU NÃO) DA CONTRATAÇÃO

16.1 Considerando todo o exposto acima, esta Secretaria de Tecnologia da Informação e Comunicação declara que a contratação de solução de análise de vulnerabilidade, desenvolvimento seguro e que contemple mecanismos antifraude é fundamental e viável, diante da necessidade de garantir a continuidade da proteção de aplicações, serviços e infraestrutura crítica do TJAM, elevar o nível de maturidade em segurança cibernética e atender às demandas por automação, integração e inteligência frente às ameaças digitais modernas.

16.2 A contratação é imprescindível para assegurar a análise contínua de vulnerabilidades em aplicações e infraestrutura, proteger contra fraudes digitais (inclusive clonagem de domínios e perfis falsos), monitorar a exposição de credenciais na surface, deep e dark web, além de integrar-se nativamente às esteiras de desenvolvimento (CI/CD).

16.3 A solução atende às diretrizes normativas estabelecidas na Resolução CNJ nº 468/2022, Resolução CNJ nº 396/2021, Resolução CNJ nº 370/2021, e está alinhada à Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).

16.4 A contratação se faz essencial para garantir a eficiência, a resiliência e a segurança das operações digitais do TJAM, especialmente diante do aumento de ataques cibernéticos direcionados ao setor público. A contratação representa uma medida proativa de alto impacto na proteção dos ativos de informação e na continuidade da prestação jurisdicional.

17. OBRIGAÇÕES PERTINENTES À LEI GERAL DE PROTEÇÃO DE DADOS

17.1 A contratada deverá garantir as melhores práticas relacionadas à Segurança da Informação e à Lei Geral de Proteção de Dados Pessoais (LGPD), principalmente, no que diz respeito aos dados pessoais tratados durante a configuração dos privilégios.

17.2 A contratada, durante a execução do objeto, deve implementar medidas técnicas e administrativas adequadas para proteger os dados pessoais contra acessos não autorizados.

17.3 Será exigido da Contratada que cada profissional que venha a prestar serviços assine um termo de compromisso, pelo qual se comprometerá a manter o sigilo das informações.

17.4 A Contratada deverá manter sigilo absoluto a respeito de quaisquer dados, informações e artefatos, contidos em documentos e mídias de que venha a ter conhecimento durante a execução dos trabalhos, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de aplicação das sanções cabíveis, além do pagamento de indenização por perdas e danos, independentemente da classificação de sigilo conferido pelo TJAM a tais documentos.

17.5 Questionário padrão acerca do tratamento de dados pessoais por parte da CONTRATADA:

17.5.1 Haverá tratamento de dados pessoais?

- Sim. A solução realizará análise de vulnerabilidades em aplicações e infraestrutura, monitoramento de credenciais e busca por possíveis vazamentos em ambientes como surface, deep e dark web. Essas atividades podem envolver a coleta e processamento de e-mails corporativos, credenciais de acesso e registros de usuários internos do TJAM, que são considerados dados pessoais.

17.5.2 Quais os dados pessoais que serão tratados?

Serão tratados dados de identificação digital e credenciais vinculadas ao ambiente do TJAM, incluindo:

- Endereços de e-mail corporativo de magistrados, servidores e colaboradores;
- Usuários e senhas eventualmente expostos em bases externas (deep/dark web);

17.5.3 Quem são os titulares destes dados pessoais?

- Endereços de e-mail corporativo de magistrados, servidores e colaboradores;

17.5.4 Qual o fundamento legal aplicável para o tratamento de dados pessoais neste caso (art. 7º da Lei Geral de Proteção de Dados)

- Art. 7º, inciso II – Cumprimento de obrigação legal ou regulatória pelo controlador, considerando as exigências das Resoluções CNJ nº 468/2022, 396/2021 e 370/2021 para adoção de medidas técnicas robustas de segurança da informação.
- Art. 7º, inciso IX – Proteção do crédito, aplicável ao monitoramento de credenciais vazadas para prevenção de fraudes.
- Art. 7º, inciso VI – Exercício regular de direitos em processo judicial ou administrativo, considerando que o TJAM é um órgão do Poder Judiciário.

17.5.5 Trata-se de tratamento de dados pessoais sensíveis (art. 5º, II, da Lei Geral de Proteção de Dados)? Se sim, qual o fundamento legal aplicável para seu tratamento (art. 11º da Lei Geral de Proteção de Dados)?

- Não

17.5.6 Haverá transferência internacional dos dados pessoais tratados? Se sim, para quem?

- Não

17.5.7 Onde os dados serão armazenados e quais os procedimentos de segurança a eles aplicados?

- Em data centers em nuvem do fabricante, com criptografia de tráfego, autenticação federada (SSO), duplo fator de autenticação (2FA) e logs de auditoria em conformidade com as melhores práticas de segurança da informação.

17.5.8 Por quanto tempo os dados pessoais serão tratados?

- Os dados serão tratados durante a vigência contratual e mantidos apenas pelo tempo necessário para o cumprimento das finalidades de análise de vulnerabilidades, investigação de incidentes e emissão de relatórios técnicos.

18. MAPEAMENTO DE RISCOS

FASE: ESTUDO TÉCNICO PRELIMINAR

ID	CAUSA (DEVIDO A)	EVENTO (PODERÁ OCORRER)	CONSEQUÊNCIA (O QUE PODERÁ LEVAR A)	PROB.	IMPACTO	NÍVEL	RESPOSTA	MEDIDAS PREVENTIVAS (PARA EVITAR QUE OCORRA)	MEDIDAS DE CONTINGÊNCIA (SE OCORRER, O QUE DEVE SER FEITO)	RESPONSÁVE
R1	Falta de alinhamento entre a necessidade e o escopo técnico do ETP	Elaboração de requisitos técnicos incompletos ou divergentes	Atrasos na contratação e necessidade de revisão do ETP	3	4	Moderado	Revisar constantemente os requisitos	Reuniões de alinhamento entre a SETIC e as unidades demandantes	Ajustar rapidamente os requisitos técnicos	SETIC
R2	Subestimação dos custos e da abrangência da solução	Estimativas de valores abaixo dos preços praticados no mercado	Restrição orçamentária e necessidade de revisão do estudo técnico	2	4	Moderado	Revisão detalhada das estimativas de custo	Pesquisa de preços de mercado atualizada e ampla	Readequar o escopo e as estimativas orçamentárias	SETIC
R3	Incompleta identificação das necessidades institucionais	Definição inadequada do objeto da contratação	Necessidade de reabertura do processo ou revisão do ETP	1	4	Baixo	Revisão da descrição das necessidades	Consulta ampla às áreas usuárias e análise do planejamento estratégico	Ajustar o objeto da contratação antes da conclusão do ETP	SETIC
R4	Não contratação da Solução	Falhas na identificação de vulnerabilidades, fraudes, vazamentos de dados e ausência de segurança no ciclo de desenvolvimento	Aumento da superfície de ataque, maior risco de incidentes críticos, fraudes, vazamento de informações sensíveis, sanções regulatórias (LGPD/CNJ) e elevação do custo operacional	3	5	Alto	Garantir a contratação da solução escolhida com prioridade	Planejamento estratégico de contratação e integração dos módulos	Mitigar riscos com soluções manuais e ferramentas isoladas (alto custo e menor eficiência)	Alta Gestão

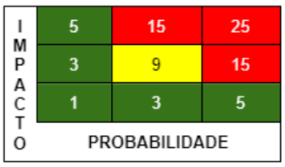
NÍVEL DE RISCO

Alto: Obrigatoriedade de tratamento do risco por meio de ação, monitoramento, e controle efetivo.

Moderado: Recomendável o tratamento do risco por meio de ação, monitoramento, e controle.

Baixo: Não há obrigatoriedade de tratamento do risco, cabendo uma reavaliação no ciclo posterior e/ou decisão da alta direção do TJAM quanto à emissão de ação, após a análise do tema em questão.

Baixo	Menor e/ou igual a 5.
Moderado	Entre 6 e 9.
Alto	Maior que 9.



Manaus, data registrada no sistema.

Washington Alves da Cunha Neto	Diogo Mendonça de Sousa	Breno Figueiredo Corado
Assessor de Segurança da Informação e Proteção de Dados	Diretor da Divisão de Infraestrutura de Tecnologia da Informação e Comunicação	Secretário de Tecnologia da Informação e Comunicação
Assinado Digitalmente	Assinado Digitalmente	Assinado Digitalmente

Documento assinado eletronicamente por **WASHINGTON NETO**, **Coordenador(a)**, em 19/11/2025, às 09:31, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **BRENO FIGUEIREDO CORADO**, **Secretário(a)**, em 19/11/2025, às 09:58, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **DIOGO MENDONCA DE SOUSA**, **Diretor(a)**, em 19/11/2025, às 10:04, conforme art. 1º, III, "b", da Lei 11.419/2006.