



TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAZONAS
DOCUMENTO DE FORMALIZAÇÃO DE DEMANDA - DFD - RESOLUÇÃO Nº 64/2023
TJAM

Responsável pela elaboração: Washington Alves da Cunha Neto

Categoria do Objeto: Serviços de Segurança da Informação.

Unidade Demandante: DVITIC/SETIC

Responsável pela Unidade Demandante: Diogo Mendonça de Sousa

Nome: Diogo Mendonça de Sousa

Matrícula: 5687-1

Telefone: (92) 99239-1948

Email: mendonca.diogo@tjam.jus.br

1. Descrição do Objeto e quantidade necessária para o atendimento da demanda:

1.1 O objeto da contratação consiste na aquisição de uma solução especializada e integrada para análise e gestão de vulnerabilidades, proteção antifraude e segurança no desenvolvimento (DevSecOps), que atenda às necessidades do Tribunal de Justiça do Estado do Amazonas. A solução deverá incluir, de forma nativa, funcionalidades de análise contínua de vulnerabilidades em aplicações e infraestrutura (SAST, DAST, SCA, IaC), monitoramento de credenciais vazadas e códigos expostos, proteção contra domínios fraudulentos e aplicativos falsos, além de integração com pipelines de CI/CD e esteiras DevSecOps. Deverá ainda abranger tanto o ambiente de Data Center quanto os ciclos de desenvolvimento e operação de sistemas críticos da instituição.

1.2 A estimativa de quantidades necessárias para o atendimento do objeto são as seguintes:

1.2.1 Grupo 01 – Detecção e Mitigação de Vulnerabilidades em Aplicações (12 meses):

1.2.1.1 Item 1: 01 licença base para habilitar funcionalidades de detecção de vulnerabilidades em aplicações.

1.2.1.2 Item 2: 04 licenças para análise de até 10 aplicações cada, vinculadas à licença base.

1.2.2 Grupo 02 – Detecção e Mitigação de Vulnerabilidades em Infraestrutura (12 meses):

1.2.2.1 Item 3: 01 licença base para habilitar funcionalidades de detecção de vulnerabilidades e ativos de infraestrutura.

1.2.2.2 Item 4: 06 licenças para análise de até 500 ativos cada, vinculadas à licença base.

1.2.3 Grupo 03 – Análise de Exposição de Credenciais Vazadas (12 meses):

1.2.3.1 Item 5: 01 licença base para habilitação de recursos de detecção de vazamento de credenciais, com possibilidade de configuração de palavras-chave e domínios principais.

1.2.4 Grupo 04 – Detecção de Domínios Fraudulentos e Proteção de Marca (12 meses):

1.2.4.1 Item 6: 04 licenças para monitoramento de 01 domínio cada, com base em recursos de inteligência de ameaças, fraudes e vazamentos.

1.2.4.2 Item 7: 01 licença base para ativação dos recursos de detecção de fraude.

1.2.4.3 Item 8: 04 licenças para configuração de até 5 palavras-chave cada, vinculadas à licença base.

1.2.5 Grupo 05 – Módulo de Treinamento:

1.2.5.1 Item 9: 01 módulo de treinamento técnico voltado aos grupos 01, 02, 03 e 04, abrangendo capacitação das equipes nas funcionalidades contratadas e melhores práticas operacionais.

2. Previsão da contratação no plano de contratações anual:

2.1 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](#).

3. Justificativa para a contratação e para a quantidade

3.1 A presente contratação tem como objetivo a aquisição de uma solução integrada de análise e gestão de vulnerabilidades e ameaças cibernéticas, capaz de promover a evolução do modelo de segurança da informação adotado pelo Tribunal de Justiça do Estado do Amazonas. A necessidade da contratação decorre do atual cenário de crescente sofisticação de ataques cibernéticos direcionados ao setor público, o qual exige a adoção de medidas preventivas e reativas mais inteligentes, automatizadas e integradas, em conformidade com as boas práticas de segurança cibernética e com as diretrizes normativas aplicáveis. Embora o TJAM disponha de soluções tradicionais de proteção, sua infraestrutura tecnológica é composta por aproximadamente 500 servidores virtuais, mais de 60 comarcas, e um universo de mais de 4.500 usuários ativos, incluindo magistrados, servidores e colaboradores. Tal complexidade, somada à criticidade dos serviços prestados, torna insuficiente a utilização de abordagens isoladas ou pontuais, sendo imprescindível uma solução unificada e centralizada que proporcione visibilidade em tempo real, gestão de vulnerabilidades, resposta automatizada a ameaças e aplicação de práticas modernas como DevSecOps, integradas aos fluxos de desenvolvimento contínuo;

3.2. A contratação está em conformidade com as normativas do Conselho Nacional de Justiça, como as Resoluções CNJ nº 468/2022, 370/2021 e 396/2021, que tratam da proteção de dados pessoais, da modernização da infraestrutura tecnológica e da obrigatoriedade de controles técnicos para prevenção e resposta a incidentes de segurança, além de seguir a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ). Nesse contexto, a medida é essencial para assegurar a confidencialidade, integridade e disponibilidade dos ativos digitais do TJAM, promovendo também eficiência operacional, resiliência institucional e confiança social nos serviços judiciais.

3.3 Definição da quantidade a ser adquirida considerou a complexidade da infraestrutura de TI do TJAM, composta por centenas de servidores virtuais, redes e ambientes diversos, bem como a necessidade de cobertura abrangente da solução em todos os sistemas e ambientes (produção, homologação e desenvolvimento), incluindo varreduras na surface, deep e dark web. Também foram considerados os requisitos de integração com ferramentas e fluxos de desenvolvimento contínuo, o monitoramento proativo de riscos e exposições, além de projeções de capacidade para atender ao crescimento esperado nos próximos 12 meses.

3.4 O TJAM ainda não possui contratação anterior de solução com o mesmo escopo técnico e funcional aqui proposto. As soluções atualmente utilizadas estão segmentadas por funções específicas, como antivírus, firewall e análise de logs, mas não contemplam uma plataforma unificada de análise de vulnerabilidades, integração DevSecOps, proteção antifraude e inteligência contra ameaças cibernéticas em redes públicas e clandestinas (dark web).

4. Requisitos da contratação: descrição dos requisitos necessários e suficientes que contribuam para a análise e escolha da melhor solução para o ETP.

4.1. O objeto da contratação pretendida é 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 A natureza da contratação é continuada e essencial à segurança institucional, 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. A contratação está em consonância com as diretrizes da Resolução CNJ nº 396/2021, que estabelece a necessidade de controles técnicos e proteção robusta em ambientes digitais, bem como com a Resolução CNJ nº 468/2022, que disciplina as contratações de soluções de tecnologia da informação e comunicação no âmbito do Poder Judiciário, assegurando que tais aquisições estejam alinhadas às melhores práticas de governança, segurança e eficiência administrativa.

4.3 A vigência inicial do contrato será de 12 (doze) meses, podendo ser prorrogada por iguais e sucessivos períodos, nos termos dos arts. 105 a 107 da Lei nº 14.133/2021, conforme vantajosidade para a Administração Pública.

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

5. Descrição da solução como um todo:

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 Data Center 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 deficiências 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 Caberá à CONTRATADA a prestação dos serviços de consultoria e suporte técnico especializado a todos os produtos adquiridos ou que venham a ser utilizados pelo Tribunal de Justiça do Estado do

Amazonas no que tange a cada sistema, pelo prazo de 12 (doze) meses, compreendendo suporte telefônico, remoto e local ("on-site", caso necessário) através de banco de horas.

5.5 Os serviços serão solicitados sob demanda, mediante a abertura de chamado efetuada por técnicos do Departamento de Informática do TJAM, via chamada telefônica, por e-mail ou plataforma de chamados da CONTRATADA, de segunda a sexta-feira (8x5).

6. Resultados pretendidos:

6.1 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.

6.2 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.

6.3 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.

6.4 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.

7. Indicar o Fiscal Técnico para o objeto a ser contratado.

7.1 A ser designado pela Secretaria de Tecnologia da Informação e Comunicação (SETIC).

Manaus, 12/09/2025.

Responsável pelo Setor demandante

Setor Demandante
(assinatura eletrônica)



Documento assinado eletronicamente por **WASHINGTON NETO, Coordenador(a)**, em 22/09/2025, às 11:25, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **DIOGO MENDONCA DE SOUSA, Diretor(a)**, em 22/09/2025, às 11:28, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **BRENO FIGUEIREDO CORADO, Subsecretário**, em 23/09/2025, às 09:08, conforme art. 1º, III, "b", da Lei 11.419/2006.



A autenticidade do documento pode ser conferida no site https://sei.tjam.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2434466** e o código CRC **C78D3E87**.

