



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

1. OBJETO DA CONTRATAÇÃO

1.1. Definição do Objeto: Registro de preços para eventual aquisição de solução de análise de vulnerabilidade, desenvolvimento seguro, que contemple mecanismos antifraude, conforme condições e exigências estabelecidas neste instrumento. **CATSER: 27502**

1.2. Justificativa para a aquisição:

1.2.1. 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.

1.2.2. Demais justificativas para a aquisição encontram-se pormenorizadas em tópico específico do Estudo Técnico Preliminar, anexo deste Termo de Referência.

1.2.3. Os resultados esperados com a aquisição são:

1.2.3.1. 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.

1.2.3.2. 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.

1.2.3.3. 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.

1.2.3.4. 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.

1.3. Especificação técnica do Objeto e Quantitativo:

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\$	R\$
	2	10 aplicações para todos os recursos que utilizam aplicação.	01	04	Unidade	R\$	R\$
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\$	R\$
	4	100 ativos para todos os recursos que utilizam ativo.	01	06	Unidade	R\$	R\$
03	Análise de Exposição de Credenciais para 12 meses						
	5	Licença base para habilitar os recursos de detecção de vazamento.	01	01	Unidade	R\$	R\$
04	Detecção de Domínios Fraudulentos para 12 meses						
	6	1 domínio para todos os recursos que utilizam domínio.	01	04	Unidade	R\$	R\$
	7	Licença base para habilitar os recursos de detecção de fraude.	01	01	Unidade	R\$	R\$
	8	5 palavras-chave para todos os recursos que utilizam palavra-chave.	01	04	Unidade	R\$	R\$
05	Módulo de treinamentos						
	9	Módulo de treinamento para os grupos 01, 02, 03 e 04	01	01	Unidade	R\$	R\$
VALOR TOTAL ESTIMADO DO SRP						R\$	

1.3.1. A justifica para o quantitativo a ser adquirido encontra-se no Estudo Técnico Preliminar, anexo a este termo.

1.3.2. GRUPO 01 - Detecção e Mitigação de Vulnerabilidades em Aplicações

1.3.2.1. A solução deve permitir análise de até 10 aplicações em desenvolvimento e/ou já existentes no ambiente de produção do TJAM.

1.3.2.2. 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.

1.3.2.3. Para fins de análise do código-fonte, não deverá ser realizado envio (upload) para a nuvem da CONTRATADA ou de terceiros.

1.3.2.4. Deve ser compatível com protocolo Git com o objetivo de se conectar no repositório de código-fonte do TJAM.

1.3.2.5. 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.

1.3.2.6. 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.

1.3.2.7. 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:

1.3.2.7.1. 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.

1.3.2.7.2. Quando houver alguma vulnerabilidade considerada alta ou crítica não tratada.

1.3.2.7.3. Quando houver código sensível identificado na análise de código-fonte com objetivo de detectar e alertar sobre melhorias de qualidade de código.

1.3.2.8. A solução deve possuir funcionalidade para análise de código e detectar e alertar sobre vulnerabilidades de segurança (SAST – Static Application Security Testing).

1.3.2.9. A solução deve possuir funcionalidade para análise de segurança de terceiros (SCA – Software Composition Analysis).

1.3.2.10. A solução deve possuir funcionalidade para varredura de vulnerabilidades dinâmicas na aplicação (DAST – Dynamic Application Security Testing).

1.3.2.11. A solução deve possuir funcionalidade para varredura em containers, Docker, para detectar vulnerabilidades de segurança.

1.3.2.12. A solução deve possuir funcionalidade para análise de vulnerabilidades em aplicações móveis (MAST – Mobile Application Security Testing).

1.3.2.13. A solução deve possuir funcionalidade para análise de segurança em infraestrutura como código (IaC – Infrastructure as Code), por exemplo, Ansible e Terraform.

1.3.2.14. A solução deve ter capacidade de identificação de vulnerabilidades do OWASP TOP10.

1.3.2.15. A solução deve possuir funcionalidades para análise de código com recomendações de melhoria de qualidade.

1.3.2.16. 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).

1.3.2.17. A solução deve gerar alertas de vulnerabilidades via plataforma: e-mail, Telegram e/ou Slack.

1.3.2.18. A solução deve possuir painel (dashboard) que apresente o nível de risco de código-fonte e infraestrutura por criticidade.

1.3.2.19. 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”.

1.3.2.20. A solução deve possuir funcionalidade para classificar as vulnerabilidades como falso-positivo, a priorizar ou mitigado em outro ambiente.

1.3.2.21. A solução deve permitir análise contínua, bastante a atualização do código pelo desenvolvedor, para que a plataforma inicie a análise de código.

1.3.2.22. A solução deve permitir o cadastro manual de vulnerabilidades.

1.3.2.23. 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.

1.3.3. GRUPO 02 Detecção e Mitigação de Vulnerabilidades em Infraestrutura

1.3.3.1. A Solução deve analisar até 500 dispositivos da infraestrutura do TJAM a serem definidos pela SETIC.

1.3.3.2. 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.

1.3.3.3. Deve conter um cadastro manual de tecnologias instaladas em um ativo no inventário, com no mínimo informações como: fabricante, produto e versão.

1.3.3.4. Deve contar com funcionalidade própria de inventário automatizado dos ativos do ambiente, com suporte a inventário usando credenciais de acesso aos ativos.

1.3.3.5. Deve ser capaz de identificar ativos existentes em uma faixa (range) de rede e cadastrá-los na plataforma aos poucos.

1.3.3.6. 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.

1.3.3.7. 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).

1.3.3.8. Deve ser capaz de realizar varreduras de vulnerabilidades dos ativos identificados através do inventário, em períodos definidos no próprio sistema.

1.3.3.9. Deve possuir opção para iniciar varredura de vulnerabilidades via agendamento.

1.3.3.10. 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.

1.3.3.11. Todas as vulnerabilidades detectadas pela análise de vulnerabilidades devem ser armazenadas pela plataforma para gestão.

1.3.3.12. Armazenar, também, todas as vulnerabilidades vinculadas a uma determinada tecnologia já lida.

1.3.3.13. 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.

1.3.3.14. A solução deve gerar alertas de vulnerabilidades via plataforma: e-mail, Telegram e/ou Slack.

1.3.3.15. Deve contar com opções de notificação, para que o gestor possa selecionar quais as suas preferências para recebimento de alertas.

1.3.3.16. Deve ser capaz de integrar com ferramentas de Endpoint Detection and Response (EDR).

1.3.3.17. 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.

1.3.3.18. 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).

1.3.3.19. 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).

1.3.4. ITEM 03 – Análise de Exposição Dados e Credenciais

1.3.4.1. 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;

1.3.4.2. Detectar vazamento de credenciais com base nos domínios e palavras-chave a serem definidas em conjunto pelo TJAM e CONTRATADA.

1.3.4.3. Deve realizar busca em múltiplas fontes que monitorem surface, deep e/ou dark web.

1.3.4.4. 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.

1.3.4.5. Deve implementar formas automatizadas para a classificação dos itens que foram identificados reduzindo, sempre que possível, o esforço da análise / categorização manual.

1.3.4.6. 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.

1.3.4.7. Deve implementar monitoramento de grupos de Telegram, onde são divulgadas informações dessa natureza.

1.3.4.8. 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.

1.3.4.9. Detectar vazamento de códigos-fonte de aplicações de desenvolvimento interno, com base em palavras-chave a serem definidas em conjunto pelo TJAM e CONTRATADA.

1.3.4.10. 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.

1.3.4.11. Detectar referências (links) para os domínios e/ou palavras-chave que sinalizem uma possibilidade de vazamentos de documentos ou serviços do TJAM.

1.3.4.12. 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.

1.3.4.13. 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:

1.3.4.13.1. sob análise, para itens que foram encontrados e precisam ser verificados;

1.3.4.13.2. confiável ou resolvido, para itens que foram encontrados, mas são confiáveis ou já foram resolvidos;

1.3.4.13.3. irrelevante, para itens que foram encontrados e não representam risco ou fraude.

1.3.4.14. Possibilidade de personalizar quais colunas serão exibidas e em qual ordem serão exibidas.

1.3.4.15. 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).

1.3.5. GRUPO 04 – Detecção de Domínios Fraudulentos

1.3.5.1. 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;

- 1.3.5.2. Deve realizar monitoramento de nomes de domínio cadastrados na Internet, para identificar nomes semelhantes aos domínios monitorados (tipo de ataque também conhecido como cybersquatting).
- 1.3.5.3. Deve detectar possíveis domínios fraudulentos e permitir a notificação através da própria plataforma, e-mail, Telegram e/ou Slack.
- 1.3.5.4. Deve, sempre que possível, fornecer uma foto (screenshot) da tela (homepage) do possível domínio fraudulento.
- 1.3.5.5. Deve, sempre que possível, fornecer informações de cadastro do domínio (whois).
- 1.3.5.6. Utilizar de múltiplas inteligências (por exemplo: algoritmos de registro) para descoberta de possíveis domínios fraudulentos.
- 1.3.5.7. Consultar, no ato do registro, a legitimidade do domínio.
- 1.3.5.8. 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.
- 1.3.5.9. Deve apresentar se o site em questão tiver selo seguro (HTTPS), qual a data de expiração do certificado SSL.
- 1.3.5.10. 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.
- 1.3.5.11. 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.
- 1.3.5.12. Deve detectar possíveis aplicativos móveis falsos com o nome do TJAM, através da plataforma: e-mail, Telegram e/ou Slack.
- 1.3.5.13. A plataforma deverá executar o monitoramento periódico de tais informações de forma automatizada.
- 1.3.5.14. 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.
- 1.3.5.15. 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”.
- 1.3.5.16. 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).
- 1.3.5.17. A plataforma deverá executar o monitoramento periódico de redes sociais de forma automatizada.
- 1.3.5.18. 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.
- 1.3.5.19. Tal funcionalidade tem como objetivo identificar itens que não em categorias referenciadas anteriormente, contudo mesmo assim representem potencial risco de fraude ao TJAM.
- 1.3.5.20. 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.
- 1.3.5.21. Tal funcionalidade tem como objetivo reduzir o tempo de identificação de páginas falsas que são utilizadas pelos fraudadores.
- 1.3.5.22. 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.
- 1.3.5.23. 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:
- 1.3.5.23.1. sob análise (under analysis), para itens que foram encontrados e precisam ser verificados;
- 1.3.5.23.2. confiável (trusted) ou resolvido (solved), para itens que foram encontrados, mas são confiáveis ou já foram resolvidos;
- 1.3.5.23.3. irrelevante (irrelevant), para itens que foram encontrados e não representam risco ou fraude.
- 1.3.5.24. Possibilidade de personalizar quais colunas serão exibidas e em qual ordem serão exibidas.
- 1.3.5.25. 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).
- 1.3.6. Especificação técnica comum aos GRUPOS 01, 02, 03 e 04**
- 1.3.6.1. 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.
- 1.3.6.2. A solução contratada deverá atender, diretamente ou em composição, aos seguintes requisitos desta contratação:
- 1.3.6.2.1. 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.
- 1.3.6.2.2. A solução deverá mostrar e possibilitar a integração de funcionalidades de vulnerabilidade incluindo infraestrutura, desenvolvimento seguro (DevSecOps) e proteção de reputação.
- 1.3.6.3. A solução deve contar com uma interface web intuitiva para acesso às funcionalidades.
- 1.3.6.3.1. A plataforma deverá atender os módulos dos GRUPOS 01, 02, 03 e 04.
- 1.3.6.4. Implementar controle de acesso baseado em permissões de usuários para as funcionalidades da solução.
- 1.3.6.5. 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.
- 1.3.6.6. 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.
- 1.3.6.7. Possibilidade de configurar o segundo fator de autenticação (2FA) como obrigatório para todos os usuários que utilizam a plataforma; ou
- 1.3.6.7.1. Possibilidade de configurar o segundo fator de autenticação como não obrigatório, podendo individualmente para alguns usuários que utilizam a plataforma.
- 1.3.6.8. Possibilidade de configurar Single Sign On (SSO) para autenticação através de identidade federada com, no mínimo, as seguintes soluções:
- 1.3.6.8.1. Microsoft Active Directory Federation Services (ADFS)
- 1.3.6.8.2. Okta
- 1.3.6.9. Possibilidade de escolher o idioma de interface suportando, no mínimo, 2 idiomas: português e inglês.
- 1.3.6.9.1. Deve permitir que o usuário selecione um idioma padrão que já esteja salvo toda vez que ele abrir a solução.
- 1.3.6.10. Deve possuir uma área de consulta (referência rápida) onde o usuário realizará uma busca que inclua, no mínimo, as seguintes informações:
- 1.3.6.10.1. 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.

1.3.6.10.2. 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.

1.3.6.11. Deve disponibilizar API (Application Programming Interface) para permitir integração com outras soluções do ambiente do TJAM podendo consumir os dados gerados pela plataforma.

1.3.6.12. Deve permitir a realização de ações em lote para a classificação dos achados da plataforma, possibilitando:

1.3.6.12.1. Seleção de múltiplos itens para classificação.

1.3.6.12.2. Seleção de múltiplos itens para edição de severidade, que se estenda para um ação possível da plataforma.

1.3.6.12.3. Incluir comentários em achados, sempre que possível.

1.3.6.12.4. Seleção de múltiplos itens para ações, sempre que se tratar de uma ação possível da plataforma.

1.3.6.13. 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.

1.3.7. Especificação técnica comum aos GRUPOS 01 e 02.

1.3.7.1. 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.

1.3.7.2. Entende-se por forma centralizada, não ser necessária a instalação em cada equipamento do desenvolvedor e/ou servidor de repositório de código-fonte.

1.3.7.3. Os concentradores de análise deverão ser compatíveis, no mínimo, com as seguintes versões de Sistema Operacional:

1.3.7.3.1. Ubuntu 18.04.6 LTS (Bionic), 20.04.2 LTS (Focal) e 22.04.5 (Jammy Jellyfish).

1.3.7.4. 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.

1.3.7.5. 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.

1.3.7.6. 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.

1.3.7.7. 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.

1.3.7.8. 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:

1.3.7.8.1. Achados por categoria (possibilitando filtrar: baixas, médias, altas e críticas).

1.3.7.8.2. Total de dispositivos ou achados.

1.3.7.8.3. Total de vulnerabilidades.

1.3.7.8.4. Classificação dos achados por família.

1.3.7.8.5. 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).

1.3.7.8.6. Vulnerabilidades ou achados novos ou resolvidos por período.

1.3.7.8.7. Evolução dos achados ao longo do tempo.

1.3.7.8.8. Lista configurável com, por exemplo, os 10, 15, 20, 50 ou 100 ativos com mais vulnerabilidades no ambiente.

1.3.7.9. 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.

1.3.7.10. 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).

1.3.7.11. Deve permitir filtrar as informações das vulnerabilidades com base nas seguintes informações:

1.3.7.11.1. Severidade (crítica, alta, média e baixa).

1.3.7.11.2. Família.

1.3.7.11.3. Tecnologia.

1.3.7.11.4. Status do achado (aberto, mitigado, transferido, fechado, falso-positivo e descomissionados).

1.3.7.11.5. Nome do achado/vulnerabilidade.

1.3.7.11.6. CVSS (pontuação da família ou conformidade).

1.3.7.11.7. Marcações (Tags ou Labels).

1.3.7.11.8. Datas: item criado, item em reanálise e/ou reintervenção e/ou intervenção e data que foi fechado.

1.3.7.12. 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).

1.3.8. ITEM 05 – Módulo de Treinamento nos GRUPOS 01, 02, 03 e 04

1.3.8.1. 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

1.3.8.2. O módulo de treinamento deverá ser de no mínimo 8 horas de duração, podendo ser dividi-do em 4 horas diárias.

1.3.8.3. Poderá ser realizado de forma presencial, na estrutura do TJAM, ou remoto, a ser definido pelo TJAM.

1.3.8.4. Deverá possuir uma turma de até 10 participantes, a serem definidos pelo TJAM

1.3.8.5. 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

1.3.8.6. Os instrutores deverão possuir experiência e certificação na área de segurança da informação.

1.4. Caracterização do Objeto:

1.4.1. O objeto do presente Termo de Referência enquadra-se no conceito de serviços comuns, nos termos dos incisos XIII, Art. 6º da Lei nº 14.133/2021.

1.4.2. A contratação decorrente do Registro de Preços será realizada de acordo com a necessidade e conveniência do Tribunal de Justiça do Amazonas, mediante a emissão de requisição de fornecimento e da Nota de Empenho.

1.5. Fundamentação Legal:

1.5.1. A aquisição deverá obedecer, no que couber, ao disposto na legislação a seguir:

- a) Lei nº 14.133, de 1º de abril de 2021;
- b) Resolução n.º 64/2023, de 5 de dezembro de 2023.

1.5.2. Legislações aplicáveis ao objeto a ser contratado, no que couber:

- a) Resolução CNJ nº 468/2022.

1.6. Indicação de necessidade de apresentação de amostras, catálogos, manuais, folders ou prospectos:

1.6.1. Para este certame, não será exigida apresentação de amostras, catálogos, manuais, folders ou prospectos.

1.7. Valor estimado da contratação:

1.7.1. A estimativa de valor da contratação será discriminada no Mapa de Preços a ser elaborado pela Divisão de Compras e Operações, utilizando a tabela do item 1.3

1.8. Adequação orçamentária:

1.8.1. A aquisição pretendida está prevista no Plano de Contratação Anual 2025, sob o Código **SETIC-2025-14**.

2. CONDIÇÕES GERAIS DA CONTRATAÇÃO

2.1. O objeto deste Termo de Referência caracteriza-se como situação prevista na modalidade Pregão, sob a forma Eletrônica, nos termos do artigo 28, inciso I da, Lei nº 14.133/2021.

2.2. A presente aquisição adotará como regime de execução a Empreitada por Preço unitário.

2.3. O procedimento para a aquisição pretendida neste instrumento será regido pelo Sistema de Registro de Preços, conforme apontado na escolha da solução do Estudo Técnico Preliminar.

2.4. O critério de julgamento será o de **MENOR PREÇO**.

2.5. O critério de adjudicação da contratação será GLOBAL, por se tratar de uma contratação em que os itens possuem a mesma natureza técnica, sendo portanto interdependentes entre si.

2.6. Participação de consórcios de empresas:

2.6.1. A participação de consórcios no certame que se originará do presente Termo de Referência não será permitida, em razão da complexidade e o vulto do objeto não limitarem a participação de fornecedores aptos a executar o objeto. Os potenciais fornecedores, em sua maioria, dispõem de condições de participar isoladamente do certame e prestar a integralidade do objeto, não sendo o caso de permitir a junção de esforços de 2 (duas) ou mais empresas para a execução da contratação pretendida. Nesse caso, a possibilidade de participação de consórcios poderia limitar a competitividade do certame, uma vez que se admitiria que empresas se associassem e não disputassem individualmente o objeto da licitação.

2.7. Não será permitida a subcontratação do objeto deste Termo de Referência.

2.8. Tratamento diferenciado para Microempresas, Empresas de Pequeno Porte ou Cooperativas:

2.8.1. Aplicam-se a este certame, no que couber, as disposições constantes dos [arts. 42 a 49 da Lei Complementar nº 123, de 14 de dezembro de 2006](#).

3. REQUISITOS DO FORNECEDOR

3.1. Vistoria:

3.1.1. Para a execução do objeto, não será necessária realização de vistoria.

3.2. Qualificação Técnica:

3.2.1. Qualificação técnico-profissional:

3.2.1.1. A contratada deverá, através de declaração, informar que dispõe de no mínimo 01 profissional certificado na solução.

3.2.1.2. A comprovação desse profissional deverá ser apresentada no momento da assinatura do contrato.

3.2.2. Qualificação técnico-operacional:

3.2.2.1. Para o objeto a ser licitado, será necessária a apresentação dos seguintes documentos relativos a qualificação técnico-operacional:

3.2.2.1.1. 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.

3.2.2.1.1.1. Não será exigido um quantitativo mínimo de atestados, nem quantitativo mínimo de bens ou serviços do objeto licitado, uma vez que a análise da capacidade técnica priorizará a qualidade dos serviços já executados, a experiência com objetos similares e a adequação aos prazos e condições da licitação.

3.2.2.1.1.2. No caso de pessoa jurídica de direito público, o(s) atestado(s), declaração (ões) ou certidão(ões) deverá(ão) ser assinado(s) pelo responsável do setor competente do órgão, preferencialmente munidos de mecanismos de verificação ou autenticação.

3.2.2.1.1.3. No caso de pessoa jurídica de direito privado, o(s) atestado(s) deverá(ão) conter dados suficientes para identificação civil do declarante, com referência ao cargo/função que ocupa na empresa e formas de contato, ou munidos de mecanismos de verificação ou autenticação.

3.2.2.1.2. Apresentação de certificação de competência e de revenda autorizada da solução.

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

3.2.2.1.4. Os documentos apresentados poderão ser objeto de diligência, a critério da Administração.

3.2.3. As exigências e condições estabelecidas são pertinentes e razoáveis para a garantia de que o objeto licitado tenha a qualidade desejada.

3.2.4. As exigências relativas à capacidade técnica, seja ela de caráter técnico-profissional ou técnico-operacional, guardam amparo constitucional e não constituem, por si só, restrição indevida ao caráter competitivo de uma licitação.

4. MODELO DE GESTÃO

4.1. A fiscalização do objeto será realizada pela Secretaria de Tecnologia da Informação e Comunicação.

4.1.1. A execução do objeto deverá ser acompanhada e fiscalizada por servidor designado como responsável ou por seu substituto.

4.1.2. A Secretaria de Tecnologia da Informação e Comunicação será responsável pela avaliação da conformidade da solução, e anotará em registro próprio todas as ocorrências relacionadas à falhas ou problemas observados, determinando o que for necessário à regularização das mesmas.

4.1.3. A existência da fiscalização de nenhum modo diminui ou altera a responsabilidade do fornecedor na total execução do objeto.

4.1.4. Deverá ser mantido preposto, aceito pela CONTRATANTE, durante o período de execução do objeto, para representá-lo sempre que for necessário.

4.2. As comunicações entre o órgão e a contratada devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica (e-mail) para esse fim.

4.3. Indicação de instrumento para efetivar a contratação:

4.3.1. Será necessária a formalização de Ata de Registro de Preços.

4.3.2. O prazo de vigência da Ata de Registro de Preços, contado a partir da publicação do extrato da ata no Portal Nacional de Contratações Públicas, será de 1 (um) ano, e poderá ser prorrogado por igual período, com renovação das quantidades registradas, desde que comprovado que as condições e o preço permanecem vantajosos.

4.3.3. Os órgãos e entidades poderão aderir à ata de registro de preços na condição de não participantes, observados os seguintes requisitos:

I - apresentação de justificativa da vantagem da adesão, inclusive em situações de provável desabastecimento ou descontinuidade de serviço público;

II - demonstração de que os valores registrados estão compatíveis com os valores praticados pelo mercado;

III - prévias consulta e aceitação do órgão ou entidade gerenciadora e do fornecedor.

4.3.4. A faculdade de aderir à ata de registro de preços na condição de não participante poderá ser exercida:

I - por órgãos e entidades da Administração Pública federal, estadual, distrital e municipal, relativamente a ata de registro de preços de órgão ou entidade gerenciadora federal, estadual ou distrital; ou

4.3.5. As aquisições ou as contratações não poderão exceder, por órgão ou entidade, a 50% (cinquenta por cento) dos quantitativos dos itens do instrumento convocatório registrados na ata de registro de preços para o órgão gerenciador e para os órgãos participantes.

4.3.6. O quantitativo decorrente das adesões à ata de registro de preços não poderá exceder, na totalidade, ao dobro do quantitativo de cada item registrado na ata de registro de preços para o órgão gerenciador e órgãos participantes, independentemente do número de órgãos não participantes que aderirem.

4.4. Da necessidade de formalização de contrato:

4.4.1. 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.

4.4.2. Após a assinatura do contrato, o órgão poderá convocar o representante da empresa contratada para reunião inicial para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução da contratada, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.

4.5. Vigência contratual:

4.5.1 A vigência do contrato a ser firmado será de 12 (doze) meses, podendo ser prorrogado na forma do art. 107 da Lei nº 14.133/21.

4.6. Índice de reajuste:

4.6.1. Os preços contratados poderão ser reajustados, após solicitação da CONTRATADA, observado o interregno mínimo de 12 (doze) meses, tendo como limite máximo a variação do Índice de Custos de Tecnologia da Informação - ICTI, ocorrida nos últimos 12 (doze) meses.

4.6.2. O interregno mínimo de 12 (doze) meses será contado a partir da data orçamento estimado, assim considerada a data de conclusão da apuração do valor estimado da contratação, ou, da planilha orçamentária, independentemente da data da tabela ou sistema referencial de custos utilizado.

4.6.3. Nos reajustamentos subsequentes ao primeiro, o interregno mínimo de 12 (doze) meses será contado da data de início dos efeitos financeiros do último reajustamento ocorrido.

4.6.4. O reajuste deverá ser solicitado antes do término da atual vigência do Contrato, sob pena de preclusão.

5. OBRIGAÇÕES DA CONTRATADA E DO CONTRATANTE.

5.1. São obrigações e responsabilidades do CONTRATANTE:

5.1.1. Efetuar os pagamentos nas condições e preços pactuados.

5.1.2. Promover o acompanhamento e a fiscalização da execução do objeto, sob os aspectos quantitativos e qualitativos, anotando em registro próprio as faltas detectadas e comunicando à empresa as ocorrências de qualquer fato que, a seu critério, exija medidas por parte daquela.

5.1.3. Rejeitar, no todo ou em parte, a solução entregue em desacordo com as exigências deste Termo.

5.1.4. Notificar por escrito a ocorrência de eventuais imperfeições na execução do objeto, fixando prazo para a sua correção.

5.1.5. Proporcionar todas as facilidades para que ocorra a correta execução do objeto.

5.1.6. Comunicar qualquer irregularidade ou ilegalidade encontrada no fornecimento do objeto.

5.1.7. Prestar as informações e os esclarecimentos atinentes à execução do objeto que venham a ser solicitados.

5.1.8. Solicitar o fornecimento do objeto deste Termo de Referência.

5.1.9. Fiscalizar e acompanhar a execução da Ata de Registro de Preços.

5.1.10. Manter sigilo e confidencialidade de todas as informações – em especial os dados pessoais e os dados pessoais sensíveis – repassados em decorrência da execução contratual, em consonância com o disposto na Lei n. 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD).

5.1.11. Demais obrigações estipuladas no Contrato.

5.2. São obrigações e responsabilidades da CONTRATADA:

5.2.1. Executar o objeto desta contratação, atendendo às especificações estabelecidas neste Termo de Referência e as quantidades indicadas no instrumento contratual.

5.2.2. Manter todas as condições de habilitação e qualificação exigidas na licitação em compatibilidade com as obrigações assumidas.

5.2.3. Responsabilizar-se única e exclusivamente pelo pagamento de todos os encargos e demais despesas, diretas ou indiretas, decorrentes da execução do objeto do presente Termo de Referência, tais como impostos, taxas, contribuições fiscais, previdenciárias, trabalhistas, fundiárias; enfim, por todas as obrigações e responsabilidades, sem qualquer ônus adicional ao CONTRATANTE.

5.2.4. Cumprir os normativos e os procedimentos definidos pelo CONTRATANTE.

5.2.5. Primar pelo bom planejamento das atividades, utilizar as boas práticas e técnicas de governança, avaliar previamente a viabilidade técnica, os riscos e os impactos de suas ações.

5.2.6. Realizar a entrega do objeto em conformidade com o determinado pelo CONTRATANTE.

5.2.7. Comunicar às unidades do CONTRATANTE responsáveis pela fiscalização do objeto, por escrito, qualquer anormalidade, bem como atender prontamente o que lhe for solicitado e exigido.

5.2.8. Responder por todas as despesas decorrentes do fornecimento da solução.

5.2.9. Substituir a solução que, a juízo do representante do CONTRATANTE, não forem considerados satisfatórios, sem que caiba qualquer acréscimo no custo contratado.

5.2.10. Não realizar, promover e incentivar a divulgação de qualquer dado ou informação do ambiente do CONTRATANTE.

5.2.11. Manter sigilo e ciência das normas de segurança e privacidade vigentes no órgão, se responsabilizando por todos os seus empregados diretamente envolvidos na contratação.

5.2.12. Manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de interesse do CONTRATANTE ou de terceiros de que tomar conhecimento em razão da execução do objeto deste contrato, devendo orientar seus profissionais nesse sentido.

5.2.13. Tratar todas as informações a que tenha acesso, em caráter de estrita confidencialidade, não podendo, sob qualquer pretexto, divulgar, revelar, reproduzir, ou delas dar conhecimento a terceiros estranhos a esta contratação, bem como utilizá-las para fins diferentes dos previstos na presente contratação.

5.2.14. Acatar as determinações feitas pela fiscalização do CONTRATANTE no que tange ao cumprimento do objeto.

5.2.15. Prestar, de imediato, todos os esclarecimentos solicitados pela fiscalização do CONTRATANTE no que diz respeito a execução do objeto.

5.2.16. Fornecer a solução, observadas rigorosamente as especificações constantes no Termo de Referência.

5.2.17. Responder pelos vícios e defeitos da solução e assumir os gastos e as despesas que se fizerem necessários para adimplemento das obrigações decorrentes da execução do objeto.

5.2.18. Notificar, formal e tempestivamente, a CONTRANTE sobre quaisquer irregularidades e inconformidades observadas durante a execução do objeto, bem como qualquer ocorrência relativa ao comportamento de seus empregados, quando em atendimento, que venha a ser considerada prejudicial ou inconveniente para a CONTRATADA.

5.2.19. Prestar as informações e os esclarecimentos que venham a ser solicitados pelo CONTRATANTE necessários à perfeita execução do objeto.

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

5.2.21. Manter sigilo e confidencialidade de todas as informações – em especial os dados pessoais e os dados pessoais sensíveis – repassados em decorrência da execução contratual, em consonância com o disposto na Lei n. 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD):

5.2.21.1. 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.

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

5.2.21.3. 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.

5.2.21.4. 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.

5.2.22. Demais obrigações estipuladas no Contrato.

6. REGIME DE EXECUÇÃO

6.1. A execução do objeto deste Termo de Referência será por demanda.

6.1.1. Os itens tratam de serviços contínuos, de sorte que poderão ser prorrogados sucessivamente, e que serão pagos em parcela única, quando da execução do serviço, conforme Encaminhamento SETIC/DVITIC (SEI nº 2566414).

6.2. A solicitação para início da execução do objeto será com o acionamento de ARP e assinatura do contrato. A comunicação será realizada por e-mail.

6.3. O prazo máximo para entrega da solução será de até 30 dias corridos, contados do recebimento da nota de empenho.

6.3.2. O prazo de entrega estabelecido no item anterior poderá ser prorrogado desde que devidamente justificado pela empresa.

6.3.3. A justificativa de que trata o subitem anterior deverá ser enviada ao TJAM antes do encerramento do prazo de entrega e será objeto de análise e decisão pelo TJAM.

6.4. 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:

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

6.4.2. Minimizar o tempo de resposta a incidentes;

6.4.3. Reduzir a dependência de suporte externo;

6.4.4. Manter a continuidade operacional com qualidade e segurança.

6.5. O objeto deste Termo de referência será recebido da seguinte forma:

6.5.1. **Provisoriamente**, no momento da entrega do objeto, pelo responsável por seu acompanhamento e fiscalização, mediante termo detalhado e assinado pelas partes, para efeito de verificação de conformidade com as especificações e exigências constantes neste Termo. Nesta etapa, o servidor ou a comissão designada procederá o recebimento do objeto limitando-se a verificar o discriminado na Nota Fiscal, e fazendo constar no canhoto e no verso da Nota Fiscal a data da entrega, e se for o caso, as irregularidades observadas.

6.5.2. **Definitivamente**, por servidor ou comissão designada pela autoridade competente, mediante termo detalhado e assinado pelas partes, no prazo de até 10 dias úteis, contados do recebimento provisório.

6.5.3. O objeto será recusado caso não atenda as especificações técnicas solicitadas no Termo de Referência, devendo a empresa providenciar os ajustes necessários para adequação, em um prazo de 10 dias contados a partir da comunicação, quando do não aceite.

6.5.4. Nenhum prazo de recebimento ocorrerá enquanto pendente a solução de inconsistências verificadas na execução do objeto ou no instrumento de cobrança.

6.5.5. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do objeto.

6.6. Serviços de Manutenção ou assistência técnica:

6.6.1. 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.

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

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

7. PENALIDADES POR DESCUMPRIMENTO CONTRATUAL

7.1. Poderão ser aplicadas à CONTRATADA que incorrer nas infrações previstas neste Termo de Referência, no Edital de Licitação e no Contrato Administrativo e/ou Ata de Registro de Preços, as seguintes sanções:

a) advertência;

b) multa;

c) impedimento de licitar e contratar;

d) declaração de inidoneidade para licitar ou contratar.

7.2. As sanções de advertência, impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar poderão ser aplicadas cumulativamente com a sanção de multa.

7.3. A sanção de impedimento de licitar e contratar com o ente federativo não poderá ser aplicada cumulativamente com a de declaração de inidoneidade.

7.4. A aplicação das sanções acima previstas não exclui a obrigação de reparação integral do dano causado à administração pública.

7.5. As infrações e sanções administrativas observarão os termos de cláusula específica da Minuta Contratual.

8. ADOÇÃO DE IMR OU ANS:

8.1. Não se aplica.

9. FORMA DE PAGAMENTO

9.1. O pagamento será efetuado em até 30 (trinta) dias, mediante apresentação da Nota Fiscal/Fatura, após ser devidamente atestada a sua conformidade pelo Fiscal designado para acompanhar e fiscalizar a execução.

9.2. O pagamento será efetuado por meio de Ordem Bancária Eletrônica em conta corrente indicada na Nota Fiscal/Fatura, devendo, para isso, ficar explícito o nome do banco, agência, localidade e número da conta corrente em que deverá ser efetivado o crédito.

9.3. Caso a CONTRATADA seja optante pelo Sistema Integrado de Pagamento de Impostos e Contribuições das Microempresas e Empresas de Pequeno Porte – SIMPLES, a mesma deverá apresentar, juntamente com a Nota Fiscal/Fatura, a devida comprovação, a fim de evitar a retenção na fonte dos tributos e contribuições, conforme legislação em vigor.

9.4. Para a efetivação do pagamento deverão ser mantidas as mesmas condições iniciais de habilitação, cumpridos os seguintes requisitos: Comprovação da regularidade fiscal da CONTRATADA para com a Fazenda Federal, Estadual e Municipal; Comprovação da regularidade fiscal da CONTRATADA relativa à Seguridade Social e ao Fundo de Garantia por Tempo de Serviço (FGTS), demonstrando situação regular no cumprimento dos encargos sociais instituídos por lei; Comprovação de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de Certidão Negativa de Débitos Trabalhistas (CNDT); Comprovação de regularidade junto ao Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis); e o Cadastro Nacional de Empresas Punidas (Cnep).

9.5. A Nota Fiscal/Fatura correspondente será examinada diretamente pelo Fiscal designado pela CONTRATANTE, o qual somente atestará a prestação do serviço contratado e liberará a referida Nota Fiscal/Fatura para pagamento quando cumpridas, pela CONTRATADA, todas as condições pactuadas.

9.6. Havendo erro na Nota Fiscal/Fatura ou circunstância que impeça a liquidação da despesa, aquela será devolvida pelo Fiscal à CONTRATADA e o pagamento ficará pendente até que a mesma providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento será interrompido e reiniciado a partir da regularização da situação ou reapresentação do documento fiscal, não acarretando qualquer ônus para o CONTRATANTE.

9.7. O pagamento observará, ainda, as demais disposições contidas em Cláusula específica da Minuta Contratual.

9.8. Considerando que a execução dos serviços será sob demanda, os pagamentos serão realizados para os itens efetivamente prestados, mediante apresentação da Nota Fiscal da empresa.

10. GARANTIA CONTRATUAL

10.1. A CONTRATADA deverá apresentar ao CONTRATANTE, em até 05 (cinco) dias úteis, contados da assinatura do contrato, comprovante de garantia, no valor correspondente a 5% (cinco por cento) do valor total do contrato, cabendo-lhe optar por uma das modalidades de garantia prevista no art. 96, § 1º da Lei n.º 14.133/2021.

10.2. A garantia deverá ser prestada com vigência de 03 (três) meses após o término da vigência do Contrato e será restituída automaticamente, ou por solicitação, no prazo de até 60 (sessenta) dias contados do final da vigência do contrato ou da rescisão, somente após comprovação de que a empresa pagou todas as verbas rescisórias trabalhistas decorrentes da contratação.

10.2.1. Caso a CONTRATADA não efetive o cumprimento das obrigações previstas no subitem anterior, a garantia será utilizada para o pagamento dessas verbas trabalhistas diretamente pelo CONTRATANTE.

10.3. A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:

10.3.1. Prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;

10.3.2. Multas moratórias e punitivas aplicadas pela Administração à contratada; e

10.3.3. Obrigações trabalhistas e previdenciárias de qualquer natureza e para com o FGTS, não adimplidas pelo contratado, quando couber.

10.4. Quando a garantia for apresentada em dinheiro, ela será atualizada monetariamente, conforme os critérios estabelecidos pela instituição bancária em que for realizado o depósito.

10.5. Quando a opção da garantia for a modalidade de seguro-garantia, a apólice deverá conter cláusulas específicas, oferecendo cobertura para despesas com obrigações contratuais e riscos trabalhistas, bem como multas que tenham caráter punitivo.

10.6. Aditado o Contrato, prorrogado o prazo de sua vigência ou alterado o seu valor, fica a CONTRATADA obrigada a apresentar garantia complementar ou substituí-la, no mesmo percentual e modalidades constantes desta cláusula. Nesses casos, a garantia será liberada após a apresentação da nova garantia e da assinatura do termo aditivo ao Contrato.

10.7. Nas hipóteses em que a garantia for utilizada total ou parcialmente – como para corrigir quaisquer imperfeições na execução do objeto do contrato ou para reparar danos decorrentes da ação ou omissão da CONTRATADA, de seu preposto ou de quem em seu nome agir, ou ainda nos casos de multas aplicadas depois de esgotado o prazo recursal – a CONTRATADA deverá, no prazo de 03 (três) dias, recompor o valor total dessa garantia, sob pena de aplicação de penalidades previstas neste Contrato.

10.8. O contrato oferece maior detalhamento das regras que serão aplicadas em relação à garantia da contratação.

11. CLÁUSULAS GERAIS DE SUSTENTABILIDADE

11.1. A empresa contratada deverá contribuir para a promoção do desenvolvimento nacional sustentável, em conformidade com o artigo 225 da Constituição Federal de 1988 e o artigo 5º da Lei nº 14.133/21, observando os princípios da eficiência, economicidade e sustentabilidade ambiental, social e econômica.

11.2. Adicionalmente, a contratada deverá, sempre que viável, observar as normas vigentes relacionadas à sustentabilidade ambiental e aderir às melhores práticas delineadas no Guia Prático de Critérios de Sustentabilidade para Compras no TJAM e no Guia Nacional de Contratações Sustentáveis da AGU, durante a execução dos serviços.

11.3. Cabe à contratada demonstrar ações para reduzir emissões de gases de efeito estufa em suas operações, como investir em tecnologias e práticas que reduzam o consumo de energia, adotar práticas de gestão adequada de resíduos, promover práticas de governança sustentável, reduzir o consumo de combustíveis fósseis e seus derivados.

11.4. Recomenda-se que a contratada cumpra as cotas raciais, de gênero e de pessoas com deficiência, conforme estabelecido pela legislação vigente, incluindo o Decreto Federal nº 11.430/2023.

11.5. Recomenda-se exigir da contratada um programa interno de treinamento visando à redução de consumo de energia elétrica, consumo de água e produção de resíduos sólidos, alinhado às melhores práticas de sustentabilidade.

11.6. Incentivar a adoção de tecnologias limpas e processos produtivos eficientes, visando à redução do impacto ambiental e ao uso racional dos recursos naturais.

12. RESPONSÁVEIS PELO TERMO DE REFERÊNCIA

12.1. Subscrevem o Termo de Referência os servidores responsáveis por sua elaboração, nos moldes e parâmetros estabelecidos pelo Tribunal de Justiça do Estado do Amazonas. Além da exigência legal da aprovação da autoridade competente, o instrumento em tela carece da ratificação de que retrata o que fora ordenado aos responsáveis por sua elaboração.

13. DOS ANEXOS

13.1. São partes integrantes deste Termo de Referência os seguintes anexos:

a) Mapa de Gerenciamento de Riscos na Contratação;

b) Estudo Técnico Preliminar;

c) Mapa de Preços.

Manaus, data do sistema

Karla Rozeana Bau Zarth

Seção de Elaboração de Artefatos da Contratação



Documento assinado eletronicamente por **Karla Rozeana Bau Zarth, Servidor**, em 10/12/2025, às 08:37, 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 **2612311** e o código CRC **3956FDEB**.



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

ANEXO

MAPA DE GERENCIAMENTO DE RISCOS DA CONTRATAÇÃO

CONTRATAÇÃO:	Registro de preços para eventual aquisição de solução de análise de vulnerabilidade, desenvolvimento seguro, que contemple mecanismos antifraude
OBJETIVO DA CONTRATAÇÃO:	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. 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. 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. 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.
FASE:	Termo de Referência/Projeto Básico

FASE: TERMO DE REFERÊNCIA/PROJETO BÁSICO									
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)
R1	Ausência de planejamento da Administração	Demanda não incluída no PCA (continuada ou inédita)	Desperdício de recursos públicos	1	5	Baixo	Revisão constante do PCA	Divulgação a respeito da necessidade de inclusão das demandas no PCA	Unidade requisitante solicita inclusão da demanda no PCA (se ainda houver tempo para os procedimentos de contratação)
R2	Ausência de padronização de especificações para objetos rotineiros	Multiplicidade de esforços para realizar contratações semelhantes	Esforço desnecessário para elaborar especificações da contratação • Repetição de erros	3	3	Moderado	Revisão das especificações técnicas	Equipe de planejamento da contratação promove padronização das especificações para aquisições que são comuns e utiliza o catálogo eletrônico de padronização	Diálogo com as unidades técnicas para ajuste das especificações
R3	Contratação direta (dispensa que não seja em razão do baixo valor ou inexigibilidade) sem adequado planejamento da contratação	• Contratos inadequados, principalmente com relação à execução do objeto e à gestão do contrato	Ilegalidade na contratação direta pelo indevido afastamento do procedimento licitatório	1	5	Baixo	Submeter o processo de contratação obrigatoriamente à Assessoria Jurídica ou setor equivalente para que sejam promovidas às análises de regularidade e conformidade, necessárias e pertinentes sobre a dispensa/inexigibilidade	Elaborar os estudos técnicos preliminares, plano de trabalho e termo de referência ou projeto básico para todas as contratações	Alta Administração determina obrigação de observância dos mesmos requisitos necessários para as contratações por meio de licitação (ETP, pesquisa de preço, etc.)
R4	Executar o processo de planejamento de forma muito simplificada para contratações de maior risco (alto valor, alto impacto nas atividades da organização)	Contratação que não produz resultados capazes de atender a necessidade pública	Recebimento de objeto que não satisfaz a necessidade	3	5	Alto	Equipe de planejamento deve adequar a profundidade das atividades de planejamento de acordo com o risco e o vulto da contratação	Unidade competente cria listagem de contratações que envolvem grande risco para a Administração (terceirização, infraestrutura de TI, etc.) e determina elaboração de mapa de risco	Administração designa gerente de riscos para integrar a equipe de planejamento de contratações inéditas, complexas ou de grande vulto
R5	Não parcelar solução cujo parcelamento é viável	Diminuição da competitividade	Aumento indevido do custo da contratação	1	5	Baixo	Realizar o parcelamento do objeto quando cabível	Equipe de planejamento da contratação apresenta justificativa expressa quanto à necessidade de agrupamento de itens	Administração solicita as devidas justificativas e indica alterações no edital, se necessário
R6	Definição de requisitos de contratação indevidos	Limitação indevida da competição	Direcionamento indevido para determinados fornecedores	1	3	Baixo	Revisão constante dos requisitos	Revisão dos artefatos de planejamento para verificar suficiência e adequação dos requisitos.	Elaboração de ETP pela equipe de planejamento da contratação, com análise do mercado e verificação das empresas que cumprem os requisitos de contratação

R7	Quantitativo subestimado	Falta de produtos ou serviços para atender a necessidade da contratação	Violação ao princípio da economicidade devido ao aumento no número de licitações para o mesmo objeto	3	3	Moderado	Equipe de planejamento apresenta justificativa para o quantitativo e encarta, se for o caso, planilhas e documentos comprobatórios dos levantamentos realizados que demonstrem o dimensionamento	Fiscal do contrato armazena dados da execução contratual de modo que a equipe de planejamento da contratação que elaborar os artefatos da próxima licitação da mesma solução ou de solução similar conte com informações de contratos anteriores	Realização de contratação emergencial se não houve tempo hábil para nova licitação
R8	Não observância do art. 48 da Lei Complementar n. 123/2006	Afastamento indevido do tratamento diferenciado para ME/EPP	Ilegalidade	1	3	Baixo	Observar a Lei Complementar n. 123/2006	Equipe de planejamento da contratação indica expressamente os motivos para não aplicar os privilégios para ME/ EPP	Retificação dos artefatos de planejamento
R9	Ausência de padronização do TR/PB ou Edital	Multiplicidade de esforços para realizar licitações de objetos correlatos	Divergências textuais entre o TR/PB, o edital, a minuta de contrato ou de ata	1	3	Baixo	Elaboração de documentos padronizados	Equipe de planejamento da contratação utiliza documentos padrão e indica eventuais alterações realizadas a fim de facilitar a conferência pela Assessoria Jurídico-Administrativa da Presidência	Conferência dos modelos padronizados pela alta administração
R10	Ausência de previsão de consequências para a contratada caso não mantenha as condições de habilitação exigidas na licitação	Não manutenção das condições de habilitação exigidas na licitação	Retorno de todos os riscos que foram mitigados por meio dos critérios de habilitação e qualificação da licitação	3	3	Moderado	Elaboração de documentos padronizados	Adoção de modelos de editais que estabeleçam a obrigação da contratada de manter, durante toda a execução do contrato, todas as condições de habilitação e qualificação exigidas na licitação	Administração elabora minutas de edital e de contrato padrão que contenham cláusulas de penalidades

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.

I
M
P
A
C
T
O

5	15	25
3	9	15
1	3	5

PROBABILIDADE



Documento assinado eletronicamente por **Karla Rozeana Bau Zarth, Servidor**, em 10/12/2025, às 08:37, 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 **2614725** e o código CRC **2C3289E4**.



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.º 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 Intelligence	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.
- 5.5.1.4 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.º 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
04	Detecção de Domínios Fraudulentos para 12 meses						
	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
05	Módulo de treinamentos						
	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)	RESPONSÁVEL	PRAZO	MONITORAMENTO
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	Durante a elaboração do ETP	Acompanhamento das atas de reunião e validações
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	Durante a elaboração do ETP	Revisão contínua das informações de mercado
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	Durante a elaboração do ETP	Validação da necessidade com os gestores
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	Durante a vigência do contrato atual	Acompanhamento contínuo do andamento deste processo de contratação

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

Moderado

Alto

Menor e/ou igual a 5.

Entre 6 e 9.

Maior que 9.

I	5	15	25
M	3	9	15
P	1	3	5
A			
C			
T			
O			

PROBABILIDADE

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.



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 **2565810** e o código CRC **AC9632D0**.



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

MAPA DE PREÇOS

MAPA DE PREÇOS												
GRUPO 1 (Detecção e Mitigação de Vulnerabilidades em Aplicações para 12 meses)												
ITEM	MATERIAL	UND.	QTD.	VALOR UNITÁRIO ESTIMADO		MÉDIA	DESVIO PADRÃO	LIMITE INFERIOR	LIMITE SUPERIOR	VALOR UNITÁRIO À LICITAR	VALOR TOTAL ESTIMADO A LICITAR	METODOLOGIA DE CÁLCULO APLICADA
				EMPRESA	PREÇO							
1	Licença base para habilitar os recursos de vulnerabilidade de aplicações	UN	1	FORNECEDOR 1: CLEAR TECNOLOGIA 30.088.923/0001-08	57.683,78	R\$ 53.020,95	R\$ 25.978,81	R\$ 27.042,14	R\$ 78.999,76	R\$ 65.694,59	R\$ 65.694,59	DESVIO PADRÃO
			FORNECEDOR 2: ITWARE SOLUÇÕES 04.760.042/0001-81	70.400,00								
			FORNECEDOR 3: HS PREVENT 09.052.214/0001-86	15.000,00								
			FORNECEDOR 4: INB TECNOLOGIA 50.729.499/0001-40	69.000,00								
2	10 aplicações para todos os recursos que utilizam aplicação. Requer uma licença base: aplicação	UN	4	FORNECEDOR 1: CLEAR TECNOLOGIA 30.088.923/0001-08	236.672,58	R\$ 198.732,13	R\$ 131.738,44	R\$ 66.993,69	R\$ 330.470,57	R\$ 263.824,19	R\$ 1.055.296,76	DESVIO PADRÃO
			FORNECEDOR 2: ITWARE SOLUÇÕES 04.760.042/0001-81	269.800,00								
			FORNECEDOR 3: HS PREVENT 09.052.214/0001-86	3.455,95								
			FORNECEDOR 4: INB TECNOLOGIA 50.729.499/0001-40	285.000,00								
TOTAL ESTIMADO GRUPO 1												R\$ 1.120.991,35
GRUPO 2 (Detecção e Mitigação de Vulnerabilidades em Infraestrutura para 12 meses)												
3	Licença base para habilitar os recursos de ativos e vulnerabilidades de ameaças.	UN	1	FORNECEDOR 1: CLEAR TECNOLOGIA 30.088.923/0001-08	13.184,86	R\$ 11.828,95	R\$ 6.432,35	R\$ 5.396,60	R\$ 18.261,30	R\$ 14.978,29	R\$ 14.978,29	DESVIO PADRÃO
			FORNECEDOR 2: ITWARE SOLUÇÕES 04.760.042/0001-81	16.250,00								
			FORNECEDOR 3: HS PREVENT 09.052.214/0001-86	2.380,95								
			FORNECEDOR 4: INB TECNOLOGIA 50.729.499/0001-40	15.500,00								

MAPA DE PREÇOS												
4	500 ativos para todos os recursos que utilizam ativos. Requer uma licença base: ativo	UN	6	FORNECEDOR 1: CLEAR TECNOLOGIA 30.088.923/0001-08	92.130,64	R\$ 77.002,90	R\$ 50.384,25	R\$ 26.618,65	R\$ 127.387,15	R\$ 101.943,55	R\$ 611.661,30	DESVIO PADRÃO
			FORNECEDOR 2: ITWARE SOLUÇÕES 04.760.042/0001-81	105.000,00								
			FORNECEDOR 3: HS PREVENT 09.052.214/0001-86	2.180,95								
			FORNECEDOR 4: INB TECNOLOGIA 50.729.499/0001-40	108.700,00								
TOTAL ESTIMADO GRUPO 2												R\$ 626.639,59
GRUPO 3 (Análise de Exposição de Credenciais para 12 meses)												
5	Licença base para habilitar os recursos de ativos e vulnerabilidades de ameaças.	UN	1	FORNECEDOR 1: CLEAR TECNOLOGIA 30.088.923/0001-08	49.443,24	R\$ 42.752,48	R\$ 26.109,76	R\$ 16.642,72	R\$ 68.862,24	R\$ 55.614,41	R\$ 55.614,41	DESVIO PADRÃO
			FORNECEDOR 2: ITWARE SOLUÇÕES 04.760.042/0001-81	59.900,00								
			FORNECEDOR 3: HS PREVENT 09.052.214/0001-86	4.166,66								
			FORNECEDOR 4: INB TECNOLOGIA 50.729.499/0001-40	57.500,00								
TOTAL ESTIMADO GRUPO 3												R\$ 55.614,41
GRUPO 4 (Detecção de Domínios Fraudulentos para 12 meses)												
6	1 domínio para todos os recursos que utilizam domínio. Requer uma licença base: fraude, vazamento e/ou inteligência de ameaças.	UN	4	FORNECEDOR 1: CLEAR TECNOLOGIA 30.088.923/0001-08	9.064,59	R\$ 7.929,05	R\$ 4.262,86	R\$ 3.666,19	R\$ 12.191,91	R\$ 10.031,53	R\$ 40.126,12	DESVIO PADRÃO
			FORNECEDOR 2: ITWARE SOLUÇÕES 04.760.042/0001-81	10.330,00								
			FORNECEDOR 3: HS PREVENT 09.052.214/0001-86	1.621,61								
			FORNECEDOR 4: INB TECNOLOGIA 50.729.499/0001-40	0.700,00								
7	1 domínio para todos os recursos que utilizam domínio. Requer uma licença base: fraude, vazamento e/ou inteligência de ameaças.	UN	1	FORNECEDOR 1: CLEAR TECNOLOGIA 30.088.923/0001-08	65.924,32	R\$ 56.486,48	R\$ 37.121,04	R\$ 19.365,44	R\$ 93.607,52	R\$ 74.774,77	R\$ 74.774,77	DESVIO PADRÃO
			FORNECEDOR 2: ITWARE SOLUÇÕES 04.760.042/0001-81	80.400,00								
			FORNECEDOR 3: HS PREVENT	1.621,61								

MAPA DE PREÇOS												
				09.052.214/0001-86								
				FORNECEDOR 4: INB TECNOLOGIA 50.729.499/0001-40	78.000,00							
8	1 domínio para todos os recursos que utilizam domínio. Requer uma licença base: fraude, vazamento e/ou inteligência de ameaças.	UN	4	FORNECEDOR 1: CLEAR TECNOLOGIA 30.088.923/0001-08	7.780,46	R\$ 6.825,52	R\$ 3.524,41	R\$ 3.301,11	R\$ 10.349,93	R\$ 8.560,15	R\$ 34.240,60	DESVIO PADRÃO
				FORNECEDOR 2: ITWARE SOLUÇÕES 04.760.042/0001-81	8.600,00							
				FORNECEDOR 3: HS PREVENT 09.052.214/0001-86	1.621,61							
				FORNECEDOR 4: INB TECNOLOGIA 50.729.499/0001-40	9.300,00							
TOTAL ESTIMADO GRUPO 4												R\$ 149.141,49
GRUPO 5 (Módulo de treinamentos para os itens 01, 02, 03, 04 e 05)												
9	Módulo de treinamentos para os itens 01, 02, 03, 04 e 05	UN	1	FORNECEDOR 1: CLEAR TECNOLOGIA 30.088.923/0001-08	70.000,00	R\$ 68.750,00	R\$ 20.155,64	R\$ 48.594,36	R\$ 88.905,64	R\$ 78.333,33	R\$ 78.333,33	DESVIO PADRÃO
				FORNECEDOR 2: ITWARE SOLUÇÕES 04.760.042/0001-81	80.000,00							
				FORNECEDOR 3: HS PREVENT 09.052.214/0001-86	40.000,00							
				FORNECEDOR 4: INB TECNOLOGIA 50.729.499/0001-40	85.000,00							
TOTAL ESIMADO GRUPO 5												R\$ 78.333,33
TOTAL ESIMADO DOS GRUPOS 1-5												R\$ 2.030.720,17
OBS.: OS VALORES ESTIMADOS FORAM PROVENIENTES DE PESQUISA DE MERCADO. FORNECEDOR 1: CLEAR TECNOLOGIA DA INFORMAÇÃO S.A - CNPJ: 30.088.923/0001-08 FORNECEDOR 2: ITWARE SOLUÇÕES - CNPJ : 04.760.042/0001-81 FORNECEDOR 3: HS PREVENT - CNPJ : 09.052.214/0001-86 FORNECEDOR 4: INB TECNOLOGIA - CNPJ :50.729.499/0001-40												
Manaus, 20 de Outubro de 2025. Cotado por Leonardo Lima de Abreu Assistente Judiciário THIAGO LIMA DOS SANTOS Divisão de Compras e Operações												



Documento assinado eletronicamente por **THIAGO LIMA DOS SANTOS**, Servidor, em 23/10/2025, às 10:58, 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 **2519000** e o código CRC **764B7D1**.



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

* MINUTA DE DOCUMENTO



PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAZONAS
DIVISAO DE CONTRATOS E CONVENIOS

CONTRATO ADMINISTRATIVO Nº ____/20__-FUNJEAM

CONTRATO ADMINISTRATIVO Nº ____/20__-FUNJEAM, que entre si celebram o TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAZONAS, por intermédio do FUNDO DE MODERNIZAÇÃO E REAPARELHAMENTO DO PODER JUDICIÁRIO ESTADUAL-FUNJEAM, e a empresa _____, na forma abaixo.

O TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAZONAS, por intermédio do FUNDO DE MODERNIZAÇÃO E REAPARELHAMENTO DO PODER JUDICIÁRIO ESTADUAL-FUNJEAM, sediado na Cidade de Manaus, Estado do Amazonas, à Avenida André Araújo, s/nº, Aleixo, inscrito no CNPJ/MF sob nº 04.301.769/0001-09, neste ato representado por seu Presidente, Desembargador **JOMAR RICARDO SAUNDERS FERNANDES**, neste instrumento simplesmente denominado **CONTRATANTE**, e do outro lado, a empresa **XXXXXXXXXXXXXXXXXX**, pessoa jurídica de direito privado, com seus atos constitutivos devidamente registrados na Junta Comercial do Estado **XXXXXXXXXX**, em **XX/XX/XXXX**, sob o nº **XXX**, inscrita no CNPJ/MF sob nº **XXXXXXXXXX**, estabelecida na Cidade de **XXXXXXXXXX**, Estado **XXXXXXXXXX**, à **XXXXXXXXXX**, neste ato representada pelo(a) Sr(a). **XXXXXXXXXX**, daqui por diante simplesmente denominada **CONTRATADA**, em consequência da licitação na modalidade **XXXXXXXXXX**, sob o nº **XXX/2025-COLIC/TJAM**, cuja homologação foi publicada no Diário da Justiça Eletrônico, Ano **XXX**, Edição nº **XXX**, Caderno Administrativo, em **XX/XX/XXXX**, à pág. **XX**, tendo em vista o que consta do Processo Administrativo Digital nº 2025/000022023-00, doravante referido apenas por **PROCESSO**, celebram, na presença das testemunhas adiante nominadas, o presente **CONTRATO ADMINISTRATIVO Nº XXXX/2025- FUNJEAM**, que se regerá pelas normas instituídas pela Lei 14.133/21 e suas alterações, bem como pela Resolução nº 64/2023 TJAM, ou a norma que a substituir, que a regulamenta, pelas cláusulas e condições seguintes:

CLÁUSULA PRIMEIRA – OBJETO

1.1. O objeto do presente instrumento é a contratação, sob demanda, de **serviço de aquisição de solução/licenças de análise de vulnerabilidade, desenvolvimento seguro, que contemple mecanismos antifraude**, nas condições estabelecidas no Termo de Referência.

1.2. Objeto da contratação:

GRUPO	ITEM	OBJETO	CATSER	UND.	QUANT.	VALOR UNITÁRIO	VALOR TOTAL
01	1	Licença base para habilitar os recursos de vulnerabilidade de aplicações.	27502	und.	01		
	2	10 aplicações para todos os recursos que utilizam aplicação. Requer uma licença base: aplicação	27502	und.	04		
02	3	Licença base para habilitar os recursos de ativos e vulnerabilidades de ameaças.	27502	und.	01		
	4	500 ativos para todos os recursos que utilizam ativo. Requer uma licença base: ativo.	27502	und.	06		
03	5	Licença base para habilitar os recursos de detecção de vazamento. É necessário adicionar licenças de palavra-chave e de domínio.	27502	und.	01		

04	6	1 domínio para todos os recursos que utilizam domínio. Requer uma licença base: fraude, vazamento e/ou inteligência de ameaças.	27502	und.	04		
	7	Licença base para habilitar os recursos de detecção de fraude. É necessário adicionar licenças de palavra-chave e de domínio.	27502	und.	01		
	8	5 palavras-chave para todos os recursos que utilizam palavra-chave. Requer uma licença base: fraude, vazamento e/ou inteligência de ameaças.	27502	und.	04		
05	9	Módulo de treinamentos para os grupos 01, 02, 03, 04	27502	und.	01		

1.3. Vinculam esta contratação, independentemente de transcrição, o Termo de Referência, o Edital da Licitação, a Proposta da **CONTRATADA** e os eventuais anexos destes documentos.

1.4. Estão inclusos no objeto desta contratação todo o aparato necessário à execução do objeto contratual, como o fornecimento de materiais, mão de obra, acessórios e insumos inerentes à sua execução, observando-se tipo, especificações, quantidades e condições descritas no Termo de Referência.

1.5. O regime de execução é o de empreitada por preço unitário.

CLÁUSULA SEGUNDA – LEGISLAÇÃO APLICÁVEL

2.1. O presente Contrato rege-se por toda a legislação aplicável à espécie e ainda pelas disposições que a complementarem, alterarem ou regulamentarem, cujas normas, desde já, entendem-se como integrantes do presente Termo, especialmente às normas constantes da Lei 14.133/21, a Resolução nº 64/2023 deste Tribunal de Justiça, ou outra que vier a substituí-la, e demais normas legais pertinentes.

2.2. A **CONTRATADA** declara conhecer todas essas normas e concorda em se sujeitar às estipulações, sistemas de penalidades e demais regras delas constantes, mesmo que não expressamente transcritas no presente instrumento.

CLÁUSULA TERCEIRA – VIGÊNCIA E PRORROGAÇÃO

3.1. O prazo de vigência da contratação é de 12 (doze) meses, contados da lavratura deste Contrato, prorrogável por até 10 anos, na forma do art. 106 e 107 da Lei 14.133/21.

3.2. A prorrogação de que trata este item é condicionada ao ateste, pela autoridade competente, de que as condições e os preços permanecem vantajosos para a Administração, permitida a negociação com o contratado.

3.3. É vedada a manutenção, aditamento ou prorrogação de contrato de prestação de serviços com empresa que venha a contratar empregados que sejam cônjuges, companheiros ou parentes em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de ocupantes de cargos de direção e de assessoramento, de membros ou juízes vinculados ao **CONTRATANTE**, nos termos do art. 3.º da Resolução CNJ n.º 07/2005

CLÁUSULA QUARTA – PREÇO

4.1. O valor total da contratação é de R\$ **XXXXX,XX (XXXXXX)**, perfazendo o valor mensal de R\$ **XXXXX,XX (XXXXXX)**.

4.2. No valor acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

4.3. No interesse da **CONTRATANTE** o valor deste Contrato poderá ser aumentado ou suprimido até o limite de 25% (vinte e cinco por cento), conforme disposto no artigo 125 da Lei nº 14.133/2021.

4.4. A **CONTRATADA** fica obrigada a aceitar, nas mesmas condições, os acréscimos e supressões que se fizerem necessários, até o limite ora previsto, não podendo os mesmos excederem o limite estabelecido no parágrafo anterior.

4.5. O valor acima é meramente estimativo, de forma que os pagamentos devidos ao contratado dependerão dos quantitativos efetivamente fornecidos.

CLÁUSULA QUINTA – MODELO DE EXECUÇÃO, MODELO DE GESTÃO CONTRATUAL E REEQUILÍBRIO ECONÔMICO-FINANCEIRO

5.1. O regime de execução contratual, os modelos de gestão e de execução, assim como os prazos e condições de conclusão, entrega, observação e recebimento do objeto constam no Termo de Referência, anexo a este Contrato.

5.2. O objeto contratual deverá ser executado no prazo de sua vigência.

5.3. Fica estabelecida a comunicação, preferencialmente, formal, eletrônica e escrita entre as partes, devendo a **CONTRATANTE**, sempre que comunicar/notificar a parte **CONTRATADA**, indicar prazo para acusação de recebimento do documento.

5.4 Transcorrido o prazo indicado no parágrafo anterior, presumir-se-á comunicada/notificada a **CONTRATADA** para todos os efeitos jurídicos.

5.5. A recomposição do equilíbrio econômico financeiro do contrato, além de obedecer aos requisitos previstos na Lei Federal nº 14.133/2021, será proporcional ao desequilíbrio efetivamente suportado, cuja existência e extensão deverão ser comprovados pela **CONTRATADA** ou pelo **CONTRATANTE**, conforme o caso, e darão ensejo à alteração do valor do contrato para mais ou para menos, respectivamente.

5.6. O pleito da recomposição do equilíbrio econômico-financeiro não será acolhido quando a parte interessada falhar em comprovar os requisitos previstos no item anterior, em especial nas seguintes hipóteses:

5.6.1. A efetiva elevação dos encargos não resultar em onerosidade excessiva ou não restar comprovada e quantificada por memória de cálculo a ser apresentada pela parte interessada;

5.6.2. O evento que houver dado causa ao desequilíbrio houver ocorrido em data anterior à entrega de proposta ou posterior à expiração da vigência do contrato;

5.6.3. Não for comprovado o nexo de causalidade entre o evento e a majoração dos encargos suportados pela parte interessada;

5.6.4. A parte interessada houver, direta ou indiretamente, contribuído para a majoração de seus próprios encargos, seja pela previsibilidade do evento, seja pela possibilidade de evitar a sua ocorrência;

5.6.5. A elevação dos encargos decorrer exclusivamente de variação inflacionária, hipótese já contemplada nos critérios de reajuste previstos neste instrumento.

5.7. Havendo a revisão contratual em razão da recomposição do equilíbrio econômico-financeiro, a formalização será realizada por meio de Termo Aditivo.

CLÁUSULA SEXTA – REAJUSTAMENTO

6.1. Os preços inicialmente contratados são fixos e irrevogáveis no prazo de um ano contado da data do orçamento estimado, conforme art. 92, §3º, da Lei 14.133/2021.

6.2. Após o interregno de um ano, desde que haja pedido da **CONTRATADA**, os preços iniciais serão **reajustados**, mediante a aplicação, pelo contratante, do Índice de Custos de Tecnologia da Informação - ICTI, ocorrida nos últimos 12 (doze) meses, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

6.3. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

6.4. No caso de atraso ou não divulgação do(s) índice (s) de reajustamento, o contratante pagará ao contratado a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).

6.5. Caso o(s) índice(s) estabelecido(s) para reajustamento venha(m) a ser extinto(s) ou de qualquer forma não possa(m) mais ser utilizado(s), será(ão) adotado(s), em substituição, o(s) que vier(em) a ser determinado(s) pela legislação então em vigor.

6.6. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

6.7. O reajuste poderá ser realizado por apostilamento.

CLÁUSULA SÉTIMA – RECEBIMENTO

7.1. Os **serviços** serão **recebidos provisoriamente**, no momento da entrega, pelo(a) responsável pelo acompanhamento e fiscalização do contrato, mediante termos detalhados, quando verificado o cumprimento das exigências de caráter técnico, conforme Termo de Referência.

7.1.1. O prazo da disposição acima será contado do recebimento de comunicação de cobrança oriunda da **CONTRATADA** com a comprovação da prestação dos serviços a que se refere a parcela a ser paga.

7.2. A **CONTRATADA** fica obrigado a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não atestar a última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.

7.2.1. A fiscalização não efetuará o ateste da última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.

7.2.2. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, sem prejuízo da aplicação das penalidades.

7.3. Os serviços serão **recebidos definitivamente** no prazo de 10 (dez) dias úteis, contados do recebimento provisório, por servidor ou comissão designada pela autoridade competente, após a verificação da qualidade e quantidade do serviço e consequente aceitação mediante termo detalhado.

7.4. No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, deverá ser observado o teor do art. 143 da Lei nº 14.133, de 2021, comunicando-se à empresa para emissão de Nota Fiscal no que pertine à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

7.5. Nenhum prazo de recebimento ocorrerá enquanto pendente a solução, pela **CONTRATADA**, de inconsistências verificadas na execução do objeto ou no instrumento de cobrança.

7.6. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato.

CLÁUSULA OITAVA - PAGAMENTO

8.1. O pagamento será efetuado **em parcela única à CONTRATADA**, em até 30 (trinta) dias, mediante apresentação da Nota Fiscal/Fatura, quando os serviços efetivamente prestados, após ser devidamente atestada a sua conformidade pelo Fiscal designado para acompanhar e fiscalizar a execução contratual.

8.2. O pagamento será efetuado por meio de **Ordem Bancária Eletrônica** em conta corrente indicada na Nota Fiscal/Fatura, devendo, para isso, ficar explícito o nome do banco, agência, localidade e número da conta corrente em que deverá ser efetivado o crédito.

8.3. Caso a **CONTRATADA** seja optante pelo Sistema Integrado de Pagamento de Impostos e Contribuições das Microempresas e Empresas de Pequeno Porte – SIMPLES, a mesma deverá apresentar, juntamente com a Nota Fiscal/Fatura, a devida comprovação, a fim de evitar a retenção na fonte dos tributos e contribuições, conforme legislação em vigor.

8.4. Para a efetivação do pagamento deverão ser mantidas as mesmas condições iniciais de habilitação, cumpridos os seguintes requisitos: Comprovação da **regularidade fiscal** da **CONTRATADA** para com a **Fazenda Federal, Estadual e Municipal**; Comprovação da **regularidade fiscal** da **CONTRATADA** relativa à **Seguridade Social** e ao **Fundo de Garantia por Tempo de Serviço (FGTS)**, demonstrando situação regular no cumprimento dos encargos sociais instituídos por lei; Comprovação de **inexistência de débitos inadimplidos perante a Justiça do Trabalho**, mediante a apresentação de **Certidão Negativa de Débitos Trabalhistas (CNDT)**; Comprovação de regularidade junto ao Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis); e o Cadastro Nacional de Empresas Punidas (Cnep).

8.5. A **CONTRATADA** deverá encaminhar ao **CONTRATANTE**, através do e-mail **contratos@tjam.jus.br**: a Nota Fiscal/Fatura acompanhada dos documentos previstos nesta Cláusula, bem como das certidões que comprovem a regularidade fiscal da **CONTRATADA**, **relatórios técnicos e fotográficos que comprovem a execução do objeto, se for o caso**, a fim de que sejam adotadas as medidas inerentes ao pagamento.

8.6. A Nota Fiscal/Fatura correspondente será examinada diretamente pelo Fiscal designado pela **CONTRATANTE**, o qual somente atestará a prestação do serviço contratado e liberará a referida Nota Fiscal/Fatura para pagamento quando cumpridas, pela **CONTRATADA**, todas as condições pactuadas.

8.6.1 Em nenhuma hipótese será efetuado pagamento de Nota Fiscal/Fatura com o número do CNPJ/MF diferente do que foi apresentado na proposta de preços, mesmo que sejam empresas consideradas matriz e filial ou vice versa, ou pertencentes ao mesmo grupo ou conglomerado.

8.7. Havendo erro na Nota Fiscal/Fatura ou circunstância que impeça a liquidação da despesa, aquela será devolvida pelo Fiscal à **CONTRATADA** e o pagamento ficará pendente até que a mesma providencie as medidas sancionadoras. Nesta hipótese, o prazo para pagamento será interrompido e reiniciado a partir da regularização da situação ou reapresentação do documento fiscal, não acarretando qualquer ônus para o **CONTRATANTE**.

8.8. A não disponibilização das informações e/ou documentos exigidos nesta cláusula caracteriza descumprimento de cláusula contratual, sujeitando a **CONTRATADA** à aplicação de penalidade(s) prevista(s) neste contrato.

8.9. O **CONTRATANTE** pode deduzir do montante a pagar os valores correspondentes a multas ou indenizações devidas pela **CONTRATADA**, nos termos deste contrato.

8.10. Ocorrendo atraso no pagamento, e desde que para tal não tenha concorrido de alguma forma a **CONTRATADA**, haverá incidência de atualização monetária sobre o valor devido, pela variação acumulada do Índice de Preço ao Consumidor Amplo (IPCA), publicado pelo Instituto Brasileiro de Geografia e Estatística – IBGE, ocorrida entre a data final prevista para o pagamento e a data de sua efetiva realização.

CLÁUSULA NONA - DOTAÇÃO ORÇAMENTÁRIA

9.1. As despesas com a prestação de serviços do presente Contrato serão custeadas, no exercício em curso, por conta do Programa de Trabalho _____, Elemento de Despesa _____, Fonte de Recurso _____, Unidade Orçamentária _____ (_____), Nota de Empenho _____, de ____/____/____, no valor de R\$ _____ (_____).

CLÁUSULA DÉCIMA - OBRIGAÇÕES DAS PARTES

10.1. São obrigações da **CONTRATANTE**:

- a) Exigir o cumprimento de todas as obrigações assumidas pela **CONTRATADA**, de acordo com o contrato e seus anexos;
- b) Receber o objeto no prazo e condições estabelecidas no Termo de Referência;
- c) Notificar a **CONTRATADA**, por escrito, sobre vícios, defeitos ou incorreções verificadas na execução do objeto, para que seja por ele substituído, reparado ou corrigido, no total ou em parte, às suas expensas, fixando prazo para a sua correção, certificando-se de que as soluções por ele propostas sejam as mais adequadas;
- d) Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações pela **CONTRATADA**;
- e) Efetuar o pagamento à **CONTRATADA** do valor correspondente à execução do objeto, no prazo, forma e condições estabelecidos no presente Contrato e seus anexos;
- f) Aplicar à **CONTRATADA** as sanções previstas na lei e neste Contrato;
- g) Explicitamente emitir decisão sobre todas as solicitações e reclamações relacionadas à execução do presente Contrato, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do ajuste, no prazo de 30 dias, a contar da data do protocolo do requerimento para decidir, admitida a prorrogação motivada, por igual período;
- h) Responder eventuais pedidos de reestabelecimento do equilíbrio econômico-financeiro feitos pelo contratado no prazo máximo de 30 dias, admitida a prorrogação motivada, por igual período;
- i) Prestar esclarecimentos e fornecer por escrito as informações necessárias para a execução do objeto do contrato.

j) Não responder por quaisquer compromissos assumidos pela **CONTRATADA** com terceiros, ainda que vinculados à execução do contrato, bem como por qualquer dano causado a terceiros em decorrência de ato do **CONTRATADO**, de seus empregados, prepostos ou subordinados;

k) Rejeitar, no todo ou em parte, serviço ou fornecimento executado em desacordo com este contrato e com o Termo de Referência;

10.2. São obrigações da **CONTRATADA**:

a) A **CONTRATADA** deve cumprir todas as obrigações constantes deste Contrato e em seus anexos, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto;

b) Atender às determinações regulares emitidas pelo fiscal ou gestor do contrato ou autoridade superior e prestar todo esclarecimento ou informação solicitadas;

c) Informar imediatamente à **CONTRATANTE** qualquer ocorrência anormal, acidentes, condições inadequadas, quaisquer atos ou fatos que possam ser causa de prejuízos ou transtornos à perfeita execução do objeto;

d) Comunicar, por escrito, eventual atraso ou interrupção da execução do objeto, apresentando razões justificadoras que serão objeto de apreciação pelo **CONTRATANTE**, sem prejuízo das eventuais sanções cabíveis;

e) Prestar todas as informações e esclarecimentos solicitadas pela **CONTRATANTE** no prazo por ela estabelecido, inclusive, facilitando a ação da Fiscalização na inspeção da execução dos serviços, quando for o caso, em qualquer dia ou hora;

f) Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os bens e/ou serviços nos quais se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

g) Efetuar comunicação ao **CONTRATANTE**, assim que tiver ciência da impossibilidade de entrega do bem ou realização/finalização do serviço no prazo estabelecido, para adoção de ações de contingência cabíveis;

h) Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, de acordo com o Código de Defesa do Consumidor (Lei nº 8.078, de 1990), bem como por todo e qualquer dano causado à Administração ou terceiros, não reduzindo essa responsabilidade a fiscalização ou o acompanhamento da execução contratual pelo **CONTRATANTE**, que ficará autorizado a descontar dos pagamentos devidos ou da garantia, caso exigida no edital, o valor correspondente aos danos sofridos, consoante art. 120 da Lei 14.133/2021;

i) Responsabilizar-se pelo cumprimento de todas as obrigações trabalhistas, previdenciárias, fiscais, comerciais e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade ao contratante e não poderá onerar o objeto do contrato, consoante art. 121 da Lei 14.133/2021;

j) Responsabilizar-se, integral e exclusivamente, pelas obrigações com mão de obra, materiais, transporte, refeições, uniformes, ferramentas, equipamentos, encargos sociais, trabalhistas, previdenciários, fiscais, cíveis e criminais, resultantes da execução do Contrato, inclusive no tocante aos seus empregados, dirigentes e prepostos;

k) Apresentar, sempre que solicitado, as seguintes informações e/ou os documentos listados: **Nota Fiscal/Fatura**; Comprovação da **regularidade fiscal** da **CONTRATADA** para com a **Fazenda Federal, Estadual e Municipal**; Comprovação da **regularidade fiscal** da **CONTRATADA** relativa à **Seguridade Social** e ao **Fundo de Garantia por Tempo de Serviço (FGTS)**, demonstrando situação regular no cumprimento dos encargos sociais instituídos por lei; Comprovação de **inexistência de débitos inadimplidos perante a Justiça do Trabalho**, mediante a apresentação de **Certidão Negativa de Débitos Trabalhistas (CNDT)**; Comprovação de regularidade junto ao **Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis)** e o **Cadastro Nacional de Empresas Punidas (Cnep)**;

l) Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições exigidas para habilitação na licitação;

m) Cumprir, durante todo o período de execução do contrato, a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, conforme art. 116, da Lei nº 14.133, de 2021;

n) Cumprir a reserva de cargos para menores aprendizes, nos termos do art. 92, XVII da Lei 14.133/2021, do art. 429 do Decreto-Lei nº 5.452/1943, da Resolução 64/2023 deste Tribunal de Justiça do Amazonas ou daquelas normas que vierem a substituí-las. O seu descumprimento poderá resultar nas sanções previstas nos normativos citados e neste Contrato Administrativo;

o) Cumprir a reserva de cargos para reabilitados da previdência social, nos termos do art. 92, XVII da Lei 14.133/2021, do art. 93 da Lei nº 8.213/91, da Resolução 64/2023 deste Tribunal de Justiça do Amazonas ou daquelas normas que vierem a substituí-las. O seu descumprimento poderá resultar nas sanções previstas nos normativos citados e neste Contrato Administrativo;

p) No início da contratação, quando da eventual prorrogação contratual ou sempre que a **CONTRATANTE** entender necessário, o cumprimento das reservas de cargos para menores aprendizes e para reabilitados da previdência social serão verificadas com emissão de certidão eletrônica junto ao Ministério do Trabalho e Emprego ou, caso necessário, pelo envio de declaração da **CONTRATADA**;

q) Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato;

r) É expressamente vedada à **CONTRATADA** a veiculação de publicidade acerca da contratação, salvo se houver prévia autorização do **CONTRATANTE**;

s) Sempre que a natureza da execução do objeto exigir, esta Administração promoverá reunião inicial com participação obrigatória da **CONTRATADA** para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução da contratada, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.

t) Cumprir e atender às normas relativas à Política de Prevenção e Enfrentamento do Assédio Moral, do Assédio Sexual e da Discriminação, a fim de promover o trabalho digno, saudável, seguro e sustentável no âmbito do Poder Judiciário instituídas pela Resolução nº 518 de 31/08/2023 do Conselho Nacional de Justiça (CNJ);

u) Manter preposto aceito pela Administração para representá-lo na execução do contrato;

v) A indicação ou a manutenção do preposto da empresa poderá ser recusada por este Tribunal de Justiça do Amazonas, desde que devidamente justificada, devendo a empresa designar outro para o exercício da atividade;

w) Informar contatos (e-mails, telefones e endereços de correspondência) do(s) preposto(s) técnico e administrativo, previamente aceito pela **CONTRATANTE** para representar a **CONTRATADA** sempre que for necessário;

x) 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;

y) 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;

z) Observar e cumprir todas as demais obrigações previstas no Termo de Referência não descritas nesta cláusula.

CLÁUSULA DÉCIMA PRIMEIRA - OBRIGAÇÕES PERTINENTES À LEI GERAL DE PROTEÇÃO DE DADOS

11.1. As cláusulas seguintes são aplicáveis ao tratamento de dados pessoais, conforme especificado no Termo de Referência.

11.2. As partes deverão cumprir a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados), quanto a todos os dados pessoais a que tenham acesso em razão deste Contrato Administrativo, a partir da apresentação da proposta no procedimento de contratação, independentemente de declaração ou de aceitação expressa.

11.3. A **CONTRATADA** terá acesso aos dados pessoais que estão de posse da **CONTRATANTE** apenas para as finalidades definidas pela **CONTRATANTE**, conforme especificado no Termo de Referência.

11.4. A **CONTRATADA** deve tratar os dados pessoais que tiver acesso apenas de acordo com as instruções documentadas da **CONTRATANTE**, durante a vigência do contrato, e em conformidade com estas cláusulas, e que, na eventualidade, não conseguir seguir as instruções ou de não mais poder cumprir estas obrigações, por qualquer razão, deve oficiar de modo formal este fato imediatamente à **CONTRATANTE**, sob pena de rescisão do contrato que terá o direito de rescindir o contrato sem qualquer ônus, multa ou encargo.

11.5. É dever da **CONTRATADA** orientar e treinar seus empregados sobre os deveres, requisitos e responsabilidades decorrentes da Lei Geral de Proteção de Dados.

11.6. A **CONTRATADA** deverá exigir de suboperadores e subcontratados, se houver, o cumprimento dos deveres da presente cláusula, permanecendo integralmente responsável por garantir sua observância.

11.7. A **CONTRATADA** ao tomar conhecimento de que os dados pessoais que recebeu são imprecisos ou desatualizados, deve informar a **CONTRATANTE**, sem demora injustificada. Neste caso, o **CONTRATANTE** deve apoiar a **CONTRATADA** para apagar ou retificar os dados.

11.8. No caso de uma violação de dados pessoais relativos a dados pessoais tratados pela **CONTRATADA** sob este contrato, a **CONTRATADA** deve tomar as medidas apropriadas para lidar com a violação, incluindo medidas para mitigar seus efeitos adversos. A **CONTRATADA** também deve notificar a **CONTRATANTE** sem demora injustificada, e no prazo de 24 horas, logo após tomar conhecimento da violação. Esta notificação deve conter os detalhes de um ponto de contato, onde mais informações podem ser obtidas, uma descrição da natureza da violação (incluindo, sempre que possível, categorias e número aproximado de titulares de dados e registros de dados pessoais em questão), suas prováveis consequências e as medidas tomadas ou propostas para resolver a violação, incluindo, quando apropriado, medidas para mitigar seus possíveis efeitos adversos.

11.9. A **CONTRATADA** deve apoiar e auxiliar a **CONTRATANTE** para permitir que a mesma cumpra suas obrigações nos termos da Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), em particular para notificar a Autoridade Nacional de Proteção de Dados – ANPD e os titulares de dados afetados, levando em consideração a natureza do tratamento e as informações disponíveis para a **CONTRATADA**.

11.10. As Partes concordam que, a **CONTRATADA** ou o **CONTRATANTE** que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo, e as demais hipóteses em relação a responsabilidade e ressarcimento de danos serão regidos pelos arts. 42 a 45 e seus incisos da Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD).

11.11. O **CONTRATANTE** poderá realizar diligência para aferir o cumprimento dessa cláusula, devendo a **CONTRATADA** atender prontamente eventuais pedidos de comprovação formulados, esclarecimentos e/ou informações, no prazo estipulado pela **CONTRATANTE**.

11.12. Ao encerrar as atividades que fazem tratamento de dados pessoais, a **CONTRATADA** deve, à escolha do **CONTRATANTE**, apagar ou devolver os Dados Pessoais em sua posse, e apagar as cópias existentes. O tratamento pela **CONTRATADA** deve ocorrer apenas pelo período especificado no Termo de Referência. Até que os dados sejam apagados ou devolvidos, a **CONTRATADA** continuará a garantir o cumprimento do contrato, sem óbice de realização de posterior auditoria pela **CONTRATANTE**.

11.13. Quando necessário, a **CONTRATANTE** exigirá a apresentação de evidência técnica documentada (relatórios, logs, hash, screenshots) que comprove a eliminação correta dos dados pessoais tratados pela **CONTRATADA**.

11.14 O tratamento incorreto de dados pessoais ou a inobservância desta cláusula poderá implicar nas sanções administrativas previstas neste Contrato Administrativo e nas legislações pertinentes.

CLÁUSULA DÉCIMA SEGUNDA - SUBCONTRATAÇÃO

12.1. Não será admitida a subcontratação do objeto contratual.

CLÁUSULA DÉCIMA TERCEIRA - GARANTIA DE EXECUÇÃO

13.1. A **CONTRATADA** deverá apresentar ao **CONTRATANTE**, em até 05 (cinco) dias úteis, contados da assinatura do contrato, comprovante de garantia, no valor correspondente a **5% (cinco por cento) do valor total do contrato**, cabendo-lhe optar por uma das modalidades de garantia prevista no art. 96, § 1º da Lei n.º 14.133/2021.

13.2. A garantia deverá ser prestada com vigência de 03 (três) meses após o término da vigência do Contrato e será restituída automaticamente, ou por solicitação, **no prazo de até 60 (sessenta) dias contados do final da vigência do contrato ou da rescisão**, somente após comprovação de que a empresa pagou todas as verbas rescisórias trabalhistas decorrentes da contratação.

13.2.1. Caso a **CONTRATADA** não efetive o cumprimento das obrigações previstas no subitem anterior, **a garantia será utilizada para o pagamento dessas verbas trabalhistas diretamente pelo CONTRATANTE.**

13.3. A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:

13.3.1. Prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;

13.3.2. Multas moratórias e punitivas aplicadas pela Administração à contratada; e

13.3.3. Obrigações trabalhistas e previdenciárias de qualquer natureza e para com o FGTS, não adimplidas pelo contratado, quando couber.

13.4. Quando a garantia for apresentada em dinheiro, ela será atualizada monetariamente, conforme os critérios estabelecidos pela instituição bancária em que for realizado o depósito.

13.5. Quando a opção da garantia for a modalidade de seguro-garantia, a apólice deverá conter cláusulas específicas, oferecendo cobertura para despesas com obrigações contratuais e riscos trabalhistas, bem como multas que tenham caráter punitivo e, ainda, deverá ser apresentada em no mínimo de 1 (um) mês, contado da data de homologação da licitação e anterior à assinatura do contrato conforme art. 96. §3º da Lei 14.133/2021.

13.6. Aditado o Contrato, prorrogado o prazo de sua vigência ou alterado o seu valor, fica a **CONTRATADA** obrigada a apresentar garantia complementar ou substituí-la, no mesmo percentual e modalidades constantes desta cláusula. Nesses casos, a garantia será liberada após a apresentação da nova garantia e da assinatura do termo aditivo ao

Contrato.

13.7. Nas hipóteses em que a garantia for utilizada total ou parcialmente – como para corrigir quaisquer imperfeições na execução do objeto do contrato ou para reparar danos decorrentes da ação ou omissão da **CONTRATADA**, de seu preposto ou de quem em seu nome agir, ou ainda nos casos de multas aplicadas depois de esgotado o prazo recursal – a **CONTRATADA** deverá, no prazo de 03 (três) dias, recompor o valor total dessa garantia, sob pena de aplicação de penalidades previstas neste Contrato.

13.8. Além da garantia de que tratam os arts. 96 e seguintes da Lei nº 14.133/21, a presente contratação possui previsão de **garantia técnica** do serviço a ser fornecido, incluindo manutenção e assistência técnica, conforme condições estabelecidas no Termo de Referência.

13.9. A garantia de execução é independente de eventual garantia do produto prevista especificamente no Termo de Referência.

CLÁUSULA DÉCIMA QUARTA - ALTERAÇÕES CONTRATUAIS

14.1. Eventuais alterações contratuais reger-se-ão pela disciplina dos arts. 124 e seguintes da Lei nº 14.133, de 2021, bem como pela Resolução nº 64/2023, ou outra que vier a substituí-la, e seu anexo VI deste Tribunal de Justiça do Amazonas.

14.2. Registros que não caracterizam alteração do contrato podem ser realizados por simples apostila, dispensada a celebração de termo aditivo, na forma do art. 136 da Lei nº 14.133, de 2021.

CLÁUSULA DÉCIMA QUINTA - FISCALIZAÇÃO

15.1. A existência e a atuação da fiscalização pelo **CONTRATANTE** em nada restringem a responsabilidade, única, integral e exclusiva da **CONTRATADA**, no que concerne à execução do objeto do contrato.

15.2. Ficam reservados à Fiscalização o direito e a autoridade para resolver todo e qualquer caso singular, duvidoso ou omissivo, não previstos neste Contrato, no Edital de Licitação e seus anexos, e em tudo mais que, de qualquer forma, se relacione direta ou indiretamente, com objeto em questão, podendo determinar o que for necessário à regularização das faltas ou defeitos observados.

15.3 As atribuições da Fiscalização são aquelas constantes na Resolução nº 64-TJAM de 05 de dezembro de 2023, ou outra que vier a substituí-la, e no Manual de Gestão e Fiscalização de Contratos.

15.4 Compete à fiscalização técnica além de outras atribuições:

- a) Participação em reuniões iniciais, de trabalho e de conclusão da execução contratual;
- b) Verificação da conformidade da entrega de material, execução de obra ou prestação de serviço com as especificações, valor unitário ou total, quantidade e prazos estabelecidos no contrato;
- c) Registro de todas as ocorrências relacionadas à execução do contrato, indicando o necessário para regularização de falhas ou defeitos;
- d) Monitoramento constante da qualidade dos serviços, intervindo para solicitar à contratada a correção de faltas, falhas e irregularidades identificadas, mediante envio de SEP - Solicitação de Esclarecimentos e Providências ou Notificação Contratual.
- e) Registro e comunicação à Seção de Gestão Contratual das atividades realizadas e pendências observadas na execução do contrato;
- f) Manifestação sobre solicitações da contratada para prorrogação da execução/entrega do objeto contratual, abordando interesse na continuidade, prejuízos ao Tribunal decorrentes de atrasos e justificativas para a prorrogação de prazos;
- g) Elaboração e assinatura do termo de recebimento provisório, detalhando o cumprimento das exigências técnicas referentes a aquisições, obras ou serviços conforme as regras contratuais;
- h) Análise, em conjunto com o fiscal administrativo, dos documentos apresentados para pagamento, submetendo-os ao Fiscal para ateste ou notificação da contratada para regularização de impropriedades;
- i) Comunicação imediata à gestão contratual e à Assessoria Técnica de Fiscalização, sobre qualquer ocorrência ou incapacidade técnica da empresa contratada que possa prejudicar a execução nas datas estabelecidas;
- j) Proposição à Seção de Gestão Contratual e à Assessoria Técnica de Fiscalização, em caso de descumprimento contratual, da aplicação de sanções à contratada, conforme as regras do ato convocatório e/ou contrato, seguindo os procedimentos estabelecidos na Resolução nº 64, de 05 de dezembro de 2023, ou outra que vier a substituí-la;
- k) Elaboração, quando necessário, de relatórios, laudos e pareceres referentes às atividades de fiscalização técnica da execução do contrato;
- l) Realização de vistorias, atestando o cumprimento de orientações técnicas e indicações de segurança;
- m) Assistência à Seção de Gestão Contratual com informações necessárias para elaborar o documento comprobatório da avaliação realizada na fiscalização do cumprimento de obrigações assumidas pelo contratado;
- n) Execução de outras atribuições derivadas das cláusulas e especificidades contratuais.

CLÁUSULA DÉCIMA SEXTA - INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

16.1. O processamento e julgamento das infrações e sanções administrativas que incorrer a **CONTRATADA** tramitarão na forma de Processo Administrativo Sancionatório (PAS), consoante as normas previstas no Anexo VIII da Resolução 64/2023 deste Tribunal de Justiça do Amazonas, ou outra que vier a substituí-la.

16.2. Poderão ser aplicadas à **CONTRATADA** que incorrer nas infrações previstas neste Contrato as seguintes sanções:

- a) **Advertência;**
- b) **Impedimento de licitar e contratar;**
- c) **Declaração de inidoneidade para licitar e contratar;**
- d) **Multa** de 0,5% a 30% do valor do contrato.

16.3. Comete infração administrativa, nos termos dos artigos 155 e 156 da Lei nº 14.133, de 2021, a **CONTRATADA** que incorrer nas seguintes infrações, cabendo-a as respectivas sanções:

a) **Der causa à inexecução parcial do contrato;**

Sanções: Advertência e/ou Multa compensatória de 20% (vinte por cento) sobre o valor da parcela não cumprida, observando que o valor final apurado não poderá ser inferior a 0,5% do valor total do contrato.

b) **Der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;**

Sanções: Impedimento de licitar/contratar ou Declaração de inidoneidade para licitar/contratar e/ou Multa compensatória de 20% (vinte por cento) sobre o valor da parcela não cumprida, observando que o valor final apurado não poderá ser inferior a 0,5% do valor total do contrato.

c) **Der causa à inexecução total do contrato;**

Sanções: Impedimento de licitar/contratar ou Declaração de inidoneidade para licitar/contratar e/ou Multa compensatória de 30% do valor do contrato.

d) Ensajar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;

Sanções: Impedimento de licitar/contratar ou Declaração de inidoneidade para licitar/contratar e/ou Multa compensatória.

e) Apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;

Sanções: Declaração de inidoneidade para licitar/contratar e/ou Multa compensatória.

f) Praticar ato fraudulento na execução do contrato;

Sanções: Declaração de inidoneidade para licitar/contratar e/ou Multa compensatória.

g) Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

Sanções: Declaração de inidoneidade para licitar/contratar e/ou Multa compensatória.

h) Praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013;

Sanções: Declaração de inidoneidade para licitar/contratar e/ou Multa compensatória.

i) Inobservância dos prazos contratuais;

Sanção: Multa moratória, nos percentuais previstos no art. 18 do Anexo VIII da Resolução 64/2023 deste Tribunal de Justiça do Amazonas, ou outra que vier a substituí-la.

f) Inobservância do prazo fixado para apresentação, suplementação ou reposição da garantia, quando houver previsão contratual de sua exigência.

Sanção: Multa moratória, nos percentuais previstos no art. 18 do Anexo VIII da Resolução 64/2023 deste Tribunal de Justiça do Amazonas, ou outra que vier a substituí-la.

16.4. Na aplicação das sanções serão considerados, conforme o art. 156, §1º, da Lei nº 14.133, de 2021):

- a) A natureza e a gravidade da infração cometida;
- b) As peculiaridades do caso concreto;
- c) As circunstâncias agravantes ou atenuantes;
- d) Os danos que dela provierem para o Tribunal;
- e) A implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle;

16.5. A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa à **CONTRATADA**, observando-se o procedimento previsto no caput e parágrafos do art. 158 da Lei nº 14.133, de 2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.

16.6. Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação, conforme art. 157, da Lei nº 14.133, de 2021.

16.7. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo **CONTRATANTE** à **CONTRATADA**, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente, conforme art. 156, §8º, da Lei nº 14.133, de 2021.

16.8. Excepcionalmente, *ad cautelam*, o **CONTRATANTE** poderá efetuar a retenção do valor presumido da multa, antes da instauração do regular procedimento administrativo. Nesta hipótese, instaurará o procedimento em até 30 (trinta) dias contados da retenção.

16.9. A personalidade jurídica do Contratado poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Contrato ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o Contratado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia, conforme art. 160, da Lei nº 14.133, de 2021.

16.10. O **CONTRATANTE** deverá, no prazo máximo 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ela aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no Cadastro Nacional de Empresas Punidas (Cnep), instituídos no âmbito do Poder Executivo Federal, conforme art. 161, da Lei nº 14.133, de 2021.

16.11. As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133/21.

CLÁUSULA DÉCIMA SÉTIMA - EXTINÇÃO CONTRATUAL

17.1. O contrato se extingue quando vencido o prazo nele estipulado, independentemente de terem sido cumpridas ou não as obrigações de ambas as partes contraentes.

17.2. O contrato pode ser extinto antes do prazo nele fixado, sem ônus para o contratante, quando esta não dispuser de créditos orçamentários para sua continuidade ou quando entender que o contrato não mais lhe oferece vantagem.

17.3. A extinção nesta hipótese ocorrerá na próxima data de aniversário do contrato, desde que haja a notificação do contratado pelo contratante nesse sentido com pelo menos 2 (dois) meses de antecedência desse dia, consoante art. 106, § 1º, da Lei 14.133/2021.

17.4. Caso a notificação da não-continuidade do contrato de que trata este subitem ocorra com menos de 2 (dois) meses da data de aniversário, a extinção contratual ocorrerá após 2 (dois) meses da data da comunicação.

17.5. O contrato pode ser extinto antes de cumpridas as obrigações nele estipuladas, ou antes do prazo nele fixado, por algum dos motivos previstos no artigo 137 da Lei nº 14.133/21, bem como amigavelmente, assegurados o contraditório e a ampla defesa.

17.5.1. Nesta hipótese, aplicam-se também os artigos 138 e 139 da mesma Lei.

17.5.2. A alteração social ou a modificação da finalidade ou da estrutura da empresa não ensejará a rescisão se não restringir sua capacidade de concluir o contrato.

17.5.2.1 Se a operação implicar mudança da pessoa jurídica contratada, deverá ser formalizado termo aditivo para alteração subjetiva.

17.6. O termo de rescisão, sempre que possível, será precedido:

17.6.1. Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

17.6.2. Relação dos pagamentos já efetuados e ainda devidos;

17.6.3. Indenizações e multas.

17.7. A extinção do contrato não configura óbice para o reconhecimento do desequilíbrio econômico-financeiro, desde que o pedido ainda tenha ocorrido enquanto vigente a contratação, hipótese em que será concedida indenização por meio de termo indenizatório, conforme art. 131, *caput*, da Lei n.º 14.133, de 2021.

CLÁUSULA DÉCIMA OITAVA - CASOS OMISSOS

18.1. Os casos omissos serão decididos pelo **CONTRATANTE**, segundo as disposições contidas na Lei n.º 14.133, de 2021, e demais normas federais aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei n.º 8.078, de 1990 – Código de Defesa do Consumidor – e normas e princípios gerais dos contratos.

CLÁUSULA DÉCIMA NONA - PUBLICAÇÃO

19.1. Incumbirá ao **CONTRATANTE** a publicação do **instrumento contratual** no **Portal Nacional de Contratações Públicas (PNCP)**, na forma prevista no art. 94 da Lei 14.133, de 2021, bem como no respectivo **sítio oficial na Internet (Portal Eletrônico do TJAM)**, em atenção ao art. 8º, §2º, da Lei n. 12.527, de 2011, sendo, ainda, facultativa a publicação do **extrato deste Contrato no Diário da Justiça Eletrônico**, conforme dispõe o art. 4º, da Lei n.º 11.419, de 19 de dezembro de 2006.

CLÁUSULA VIGÉSIMA - OS MEIOS ALTERNATIVOS DE RESOLUÇÃO E PREVENÇÃO DE CONFLITOS

20.1. As partes submetem-se aos dispostos na Resolução 48/2024 do Tribunal de Justiça do Amazonas que regulamenta os meios alternativos de prevenção e solução de controvérsias no âmbito dos Contratos Administrativos deste Poder, bem como outras normas que vierem alterá-la ou substituí-la.

20.2. Na busca pela autocomposição, nas demandas originadas da execução dos contratos administrativos de competência do Poder Judiciário Amazonense, será utilizada a mediação como instrumento de solução adequada de controvérsias, para prevenir ou resolver todo o conflito, ou apenas parte dele que será conduzido pelo Comitê de Prevenção e Resolução Administrativa de Conflitos em matéria de Contratos Administrativos - CPRAC deste Tribunal de Justiça do Amazonas.

20.2.1 A autocomposição a que se refere o caput desta cláusula poderá ser adotada quanto a totalidade ou parcela de quaisquer direitos patrimoniais disponíveis no âmbito dos conflitos em matéria de contrato administrativo, **incluindo-se as questões relacionadas ao restabelecimento do equilíbrio econômico-financeiro do contrato, ao inadimplemento de obrigações contratuais por quaisquer das partes, ao cálculo de indenizações, ou, ainda, a celebração de negócio jurídico processual no Processo Administrativo Sancionatório (PAS).**

20.3. A solicitação de submissão de conflito ao CPRAC, iniciada por pessoa física ou jurídica interessada deverá ser encaminhada à Divisão de Contratos e Convênios, que instruirá o pedido com toda a documentação necessária à compreensão do caso e remeterá os autos à ao Desembargador Coordenador do Comitê para análise de admissibilidade.

20.4. As propostas, os documentos e as informações apresentados no âmbito do CPRAC serão confidenciais e não poderão ser utilizados pelas partes como meio de defesa e/ou prova em processo judicial.

CLÁUSULA VIGÉSIMA PRIMEIRA - FORO

21.1. Obriga-se a **CONTRATADA**, por si e seus sucessores, ao fiel cumprimento de todas as cláusulas e condições do presente Contrato e elege seu domicílio contratual, o da Comarca de Manaus, capital do Estado do Amazonas, para dirimir eventuais dúvidas originadas pelo presente Termo, com expressa renúncia a qualquer outro, por mais privilegiado que seja, consoante 92, §1º, da Lei 14.133 de 2021.

E assim, por estarem às partes justas e contratadas, foi lavrado o presente instrumento contratual, que lido e achado conforme pelas partes, vai por elas assinado para que produza todos os efeitos de Direito, na presença das testemunhas abaixo identificadas.

Desembargador(a) XXXXXXXX
Presidente do Tribunal de Justiça do Estado do Amazonas
CONTRATANTE

Sr. _____
Representante Legal da Empresa
CONTRATADA

TESTEMUNHAS:

Nome: _____ Nome: _____
Matrícula: _____ Matrícula: _____



Documento assinado eletronicamente por **Aldemir da Silva Menezes Medeiros, Diretor(a)**, em 24/11/2025, às 11:52, 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 **2581149** e o código CRC **9D1285FD**.

MINUTA