



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	Deteção 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	Deteção e Mitigação de Vulnerabilidades em Infraestrutura para 12 meses						
	3	Licença base para habilitar os recursos de	01	01	Unidade	R\$	R\$

		ativos e vulnerabilidades de ameaças.					
	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\$
Deteção de Domínios Fraudulentos para 12 meses							
04	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\$
Módulo de treinamentos							
05	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 - Deteção 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 individual ape-nas 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. Subscvem 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**.

2025/000022023-00

2612311v4