PODER JUDICIÁRIO
DO ESTADO DO ACRE

Secretaria de Tecnologia da Informação e Comunicação - SETIC
Subsecretaria de Contratações de TIC - SUCTI

TERMO DE REFERÊNCIA Nº 14/2026

Conformidade com o Guia de Contratações de TIC CNJ Versão 4.0 - Resolução CNJ nº 468/2022

Processo nº **2025-319**

Contratação de empresa para fornecimento de solução para proteção, detecção e resposta para endpoint e servidores contra ataques avançados, incluindo instalação, configuração, repasse de conhecimento, suporte técnico e garantia, para atender às necessidades do Tribunal de Justiça do Acre (TJAC).

Rio Branco/AC, 15 de Maio de 2026.

PODER JUDICIÁRIO
DO ESTADO DO ACRE

TERMO DE REFERÊNCIA Nº 14/2026

1. DO OBJETO:

1.1. Definição do Objeto

1.1.1. O objeto desta contratação refere-se à aquisição e implantação de uma ferramenta XDR (Extended Detection and Response) para endpoint e servidores do Poder Judiciário do Estado do Acre (PJAC), na modalidade de Software como Serviço (SaaS), com foco na prevenção, detecção, contenção e resposta a ameaças cibernéticas direcionadas aos dispositivos que compõem a base operacional do PJAC. O prazo de vigência do contrato será de 24 (vinte e quatro) meses.

ID	DESCRIÇÃO	UNID MEDIDA	CATSER	QTD	VALOR UNIT	VALOR TOTAL
1	Solução de proteção de Endpoints com abordagem proativa para resposta eficaz a incidentes	Por Endpoint	27502	2400		
2	Solução de proteção de Servidores com abordagem proativa para resposta eficaz a incidentes	Por Servidor	27502	100		
3	Serviço de suporte proativo, corretivo e para resposta a incidentes	Por Solução	27502	2		
4	Serviço de implantação	Por Solução	26972	2		
5	Serviço de capacitação e repasse de conhecimento	40 Horas	27502	1		

2. DO OBJETO:

2.1. Motivação

2.1.1. A contratação fundamenta-se na necessidade urgente de substituir a atual solução de antivírus tradicional do Poder Judiciário do Estado do Acre (PJAC), que se demonstra tecnicamente insuficiente diante do contemporâneo cenário de ameaças cibernéticas. A solução atual possui abordagem essencialmente reativa, baseada em assinaturas, sendo ineficaz contra ataques modernos como zero-day, ransomware avançado, movimentação lateral e ataques fileless. Considerando o alto volume de ativos tecnológicos (aproximadamente 2.700 equipamentos atendendo a cerca de 2.100 usuários) que sustentam serviços essenciais à prestação jurisdicional, a ausência de uma ferramenta avançada de Detecção e Resposta Estendida (XDR) com recursos de inteligência artificial e análise comportamental expõe a instituição a riscos graves de paralisação e comprometimento de dados sensíveis

2.2. Alinhamento Estratégico

2.2.1. O objeto da contratação está previsto no "Plano de Contratações de STIC 2026 do Poder Judiciário do Estado do Acre", conforme consta das informações básicas deste termo de referência.

2.2.2. O objeto da contratação também está alinhado com o Planejamento Estratégico do Poder Judiciário do Estado do Acre do 2026 e em consonância com o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) 2026 do Poder Judiciário do Estado do Acre, conforme demonstrado abaixo.

2.2.3. A contratação encontra consonância com à Estratégia Nacional de Segurança da Informação Cibernética do Poder Judiciário (ENSEC-PJ) instituída por meio da Resolução CNJ nº 396/2021, que tem o objetivo de aprimorar o nível de maturidade em segurança cibernética nos órgãos do Poder Judiciário, abrangendo os aspectos fundamentais da segurança da informação para o aperfeiçoamento necessário à consecução desse propósito.

2.2.4. Os objetivos da ENSEC-PJ são a base para tornar o espaço cibernético mais confiável, resistente, inclusivo e seguro e visam direcionar as ações dos órgãos do Poder Judiciário na área de segurança cibernética. Portanto, esta demanda deverá respeitar e observar os enunciados da Resolução CNJ nº 396/2021.

2.2.5. No que tange ao Planejamento Estratégico do Poder Judiciário do Estado do Acre, vislumbra-se o alinhamento aos objetivos estratégicos traçados.

No que concerne ao Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC), para os anos de 2025/2026, que tem o objetivo de detalhar e acompanhar as principais ações e o alcance das metas previstas para os indicadores de TIC do Poder Judiciário do Estado do Acre esta contratação atinge a ID 2, do Plano de Ações que apresenta a lista de indicadores e metas de TIC previsto para o período de vigência do PDTIC, como:

ID da Ação	Identificação do Dispositivo da Resolução	Descrição da Ação	Procedimentos	Área Responsável no Órgão (Coordenação)
2	Implantar programas eletrônicos conforme orientações do CNJ	-	-	SETIC

2.2.6. A solução indicada está alinhada às necessidades de negócio uma vez que permite a implementação dos controles estabelecidos e alterações que dispõe sobre o uso dos recursos de tecnologia da informação e comunicação do Poder Judiciário do Estado do Acre.

2.2.7. Esta contratação também será orientada, no que couber, as orientações e disposições contidas na Lei Geral de Proteção de Dados Pessoais, Lei Federal n° 13.70919, de 14 de agosto de 2018.

2.3. Objetivos

2.3.1. Em termos táticos e operacionais, a contratação visa garantir a defesa proativa e avançada dos endpoints (estações e servidores), minimizar os impactos de possíveis ataques cibernéticos e assegurar a disponibilidade contínua dos sistemas judiciais. Busca-se também diminuir o tempo médio de detecção (MTTD) e resposta (MTTR) a incidentes por meio da automação, além de reduzir custos associados à recuperação de ambientes em caso de ataques.

2.4. Referência aos Estudos Técnicos Preliminares

2.4.1. Este Termo de Referência foi elaborado considerando o Documento de Oficialização da Demanda (DOD) nº 9/2025 encaminhado pela Subsecretaria de Contratações de TIC (SUCTI) e os Estudos Técnicos Preliminares (ETP) nº 5/2025, constantes do Processo Administrativo Eletrônico GRP nº 2025-319.

2.5. Análise de Mercado de TIC

2.5.1.O ETP avaliou as alternativas disponíveis e concluiu pela inviabilidade do uso do Portal do Software Público Brasileiro, pois as soluções lá disponíveis não possuem arquitetura corporativa avançada e inteligência global de ameaças exigidas pela criticidade do PJAC. Foram confrontadas a Solução 1 (XDR em modalidade SaaS com suporte proativo e capacitação) e a Solução 2 (manutenção do antivírus tradicional). A Solução 1 foi definida como técnica e

economicamente a mais vantajosa, superando as limitações do antivírus e oferecendo correlação multivetorial contra ataques complexos.

2.5.2. Exemplo de Contextualização: Considerando as necessidades e requisitos da demanda, visualizou-se no mercado de TIC 2 alternativas de solução:

a) Solução 1: XDR em modalidade SaaS com suporte proativo e capacitação; e
b) Solução 2: Manutenção do antivírus tradicional

2.5.3. Em atendimento à análise comparativa e mercadológica, descrevem-se as características detalhadas das alternativas identificadas no Estudo Técnico Preliminar:

Solução 1: Aquisição de solução de segurança abrangente (Plataforma XDR) - Solução Escolhida

Aderência técnica à necessidade da demanda: A solução demonstrou total aderência aos requisitos do Poder Judiciário do Estado do Acre (PJAC), fornecendo uma defesa proativa com capacidade de prevenção, detecção, análise e resposta a ameaças cibernéticas avançadas para estações de trabalho e servidores
Ela garante a correlação de eventos, resposta automatizada a incidentes e o uso de inteligência artificial, promovendo a elevação do nível de maturidade em segurança cibernética, o que está em total conformidade com as exigências da Resolução CNJ nº 396/2021.

Ponderação econômica: Embora represente um volume de investimento inicial superior à mera manutenção de um antivírus comum, a Solução 1 possui a melhor relação custo-benefício. A relação é economicamente favorável quando se pondera os altos riscos operacionais, financeiros e reputacionais associados à potencial indisponibilidade dos sistemas judiciais críticos e ao vazamento de dados sensíveis da sociedade.

Serviços acessórios necessários: O fornecimento não se limita ao licenciamento do software em nuvem (SaaS), englobando obrigatoriamente os serviços acessórios de instalação, configuração, parametrização, transferência de conhecimento (capacitação da equipe), suporte técnico especializado (proativo e corretivo) 24x7 e garantia contínua de atualização tecnológica por um período de 24 (vinte e quatro) meses.

.

Contratações em outros entes públicos: A pesquisa referencial demonstrou que essa solução reflete as melhores práticas da Administração Pública atual. Foi adotada com êxito em contratações análogas pela Secretaria de Administração do Estado do Piauí (SEAD-PI), pela Universidade Federal do Rio Grande do Sul (UFRGS) e pelo Município de Jaboticabal/SP. Também verificou-se adesão à tecnologia semelhante pela Prefeitura de São Francisco de Paula/RS.

Solução 2: Manutenção da ferramenta atual (Antivírus Tradicional) - Solução Descartada
Aderência técnica à necessidade da demanda: A solução tradicional baseada apenas em assinaturas possui limitações tecnológicas relevantes que a tornam incapaz de proteger efetivamente o parque computacional. Há nítida ausência de análise comportamental avançada, incapacidade de resposta estruturada automatizada, e baixa visibilidade contra-ataques complexos (como movimentação lateral, zero-day e fileless).

Ponderação econômica: Apresenta, em um primeiro momento, um custo inicial mais baixo devido à sua menor complexidade tecnológica e por ser um modelo já implementado. Contudo, a manutenção dessa ferramenta expõe a instituição a riscos cibernéticos inaceitáveis, cujos potenciais danos financeiros oriundos de paralisação da prestação jurisdicional superam qualquer economia orçamentária de curto prazo.

Serviços acessórios necessários: Geralmente não abrange serviços de suporte proativo e orquestração de resposta a incidentes que são essenciais para um Centro de Operações de Segurança (SOC) futuro.

Contratações em outros entes públicos: O mercado público demonstra uma clara tendência de descontinuidade do uso de antivírus tradicionais para a proteção de ambientes de alta criticidade, reforçando a necessidade da migração para plataformas EDR/XDR.

2.5.4. A análise balizou-se em contratações públicas similares exitosas, tais como as realizadas pela Secretaria de Administração do Estado do Piauí (SEAD-PI), pela Universidade Federal do Rio Grande do Sul (UFRGS) e pelo Município de Jaboticabal/SP, que também aderiram à migração para plataformas XDR/EDR avançadas no modelo SaaS.

2.6. Benefícios e Resultados

2.6.1. A contratação da solução de proteção de endpoints e cargas de trabalho híbridas trará benefícios institucionais relevantes ao PJAC, estruturados sob quatro pilares:

- **Eficácia:** Ampliação da capacidade de prevenção, detecção e resposta a incidentes cibernéticos, reduzindo consideravelmente os riscos de indisponibilidade dos sistemas judiciais essenciais e de comprometimento de dados sensíveis
- **Eficiência:** Promoção de uma gestão centralizada e automatizada dos ativos tecnológicos, o que garantirá a redução de atividades manuais repetitivas e o melhor aproveitamento da força de trabalho da equipe de TIC do Tribunal, permitindo que esta atue com maior foco em ações estratégicas.
- **Economicidade:** Mitigação drástica de custos imprevistos decorrentes da correção de incidentes de segurança, diminuição de retrabalho técnico, e maior previsibilidade orçamentária ao longo dos 24 meses do contrato. Adicionalmente, propicia economia indireta ao garantir a correção tempestiva e preventiva de vulnerabilidades do ambiente.
- **Padronização:** Uniformização tecnológica, consolidando em uma plataforma única as políticas e controles de segurança em todo o parque, com consequente melhoria da governança e da rastreabilidade ágil de eventos

2.6.2. Em termos de resultados concretos a serem alcançados, almeja-se a redução mensurável de incidentes cibernéticos com impacto operacional negativo, a redução do tempo médio de detecção (MTTD) e do tempo de resposta (MTTR) a incidentes, a maior disponibilidade dos serviços para o jurisdicionado e a otimização dos recursos tecnológicos de infraestrutura já existentes no órgão.

2.7. Relação entre a Demanda Prevista e a Contratada

2.7.1. O dimensionamento quantitativo das licenças baseou-se em um rigoroso levantamento técnico do parque computacional em uso no Poder Judiciário do Estado do Acre, extraído das atuais plataformas de gestão (Wazuh e servidor antivírus), acrescido do provisionamento estratégico para crescimento orgânico da rede.

2.7.2. Forma de cálculo utilizada para a definição do quantitativo:

- **Item 1 (Solução de proteção de Endpoints)**, computou-se uma base instalada de 2.031 estações ativas, somada a 150 novos equipamentos recém-adquiridos pelo Processo nº 2025-410, totalizando 2.181 estações. Sobre esse montante, aplicou-se uma margem técnica de segurança de 10% (cerca de 218 licenças) correspondente ao crescimento da infraestrutura, resultando em 2.399 licenças. Para fins de otimização da gestão contratual, o número foi tecnicamente arredondado para o quantitativo de 2.400 licenças para Endpoints.
- **Item 2 (Solução de proteção para Servidores críticos)**, mapearam-se 90 servidores considerados de alta criticidade na hospedagem dos sistemas e bancos de dados judiciais. Aplicando idêntica margem de 10% para crescimento (9 licenças), chegou-se à estimativa de 99, arredondada para o teto de 100 licenças para Servidores.

- Demais itens (3,4 e 5), foram computados em relação aos itens 1 e 2.

2.7.3. Esta metodologia de segregação por camadas de criticidade e aplicação de fator de crescimento assegura a aderência ao princípio da eficiência técnica e previne a defasagem contratual, eliminando o risco de o Tribunal possuir ativos críticos sem cobertura de proteção cibernética durante a vigência do ajuste.

2.8. Impacto ambiental

2.8.1. A Contratada deverá conduzir a prestação dos serviços priorizando o uso racional e eficiente de recursos, evitando desperdícios significativos de energia elétrica, equipamentos ou insumos tecnológicos.

2.8.2. A execução contratual obedecerá aos preceitos do Plano de Logística Sustentável (PLS) do Poder Judiciário do Estado do Acre, cabendo à Contratada orientar ativamente seus especialistas técnicos quanto a boas práticas socioambientais, minimização da produção de lixo eletrônico e o descarte ecologicamente adequado de todo e qualquer resíduo residual pertinente às suas atividades no escopo deste contrato.

2.9. Impacto social e cultural

2.9.1. Todo o arcabouço da prestação de serviço deverá resguardar os compromissos normativos voltados a costumes, viabilidade de comunicação contínua (língua portuguesa para atendimento e suporte), e práticas de sustentabilidade traçadas pela Resolução CNJ nº 400/2021 do Conselho Nacional de Justiça.

2.9.2. O Contratante poderá engajar, e a Contratada deverá apoiar, a participação de seus prepostos e colaboradores terceirizados em eventos locais, campanhas institucionais ou programas de sensibilização voltados ao aperfeiçoamento da responsabilidade social e cultural patrocinados pelo PJAC ao longo do período de prestação.

2.10. Conformidade Legal

2.10.1. Em total respeito aos princípios balizadores da Administração Pública, a solução de XDR em Nuvem e seus serviços adjacentes pautam-se pelos preceitos da Constituição Federal de 1988 e regem-se pela Nova Lei de Licitações e Contratos Administrativos (Lei nº 14.133/2021).

2.10.2. Do ponto de vista de Governança Digital e Sistemas, a contratação cumpre estritamente a Resolução CNJ nº 468/2022, e as premissas da Instrução Normativa SGD/ME nº 94/2022 e IN SEGES/ME nº 65/2021, no que lhes forem aplicáveis.

2.10.3. Por se tratar de tratamento centralizado de logs, tráfego de dados e arquivos corporativos, a segurança da informação é fundamentada pela Estratégia Nacional de Segurança Cibernética do Poder Judiciário - ENSEC-PJ (Resolução CNJ nº 396/2021), pelo Marco Civil da Internet (Lei nº 12.965/2014) e resguarda, obrigatoriamente, conformidade total com a Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018), em sintonia fina com as demais normas de Políticas de Segurança da Informação adotadas pelo PJAC.

3. DA LICITAÇÃO:

3.1. Da Prestação da Contratação

3.1.1. O objeto desta contratação refere-se ao fornecimento de solução integrada de segurança cibernética para proteção de Endpoints e Servidores (Plataforma XDR - Extended Detection and Response), com abordagem proativa para resposta eficaz a incidentes, disponibilizada na modalidade de Software como Serviço (SaaS). A contratação abrange o licenciamento da ferramenta, serviços de suporte proativo e corretivo, serviços de implantação e serviços de capacitação (repasse de conhecimento). O prazo de vigência do contrato será de 24 (vinte e quatro) meses, contados a partir da data de sua assinatura

3.2. Da Natureza do Objeto da Contratação

3.2.1. A natureza do objeto caracteriza-se como despesa corrente, consistindo na prestação de serviço comum e continuado. A classificação como serviço continuado justifica-se pela essencialidade e habitualidade da proteção cibernética: a segurança de endpoints, servidores, rede e e-mail não pode sofrer interrupção ou descontinuidade, pois qualquer paralisação traria impacto imediato, grave e irreparável ao andamento das atividades jurisdicionais e administrativas do TJAC, deixando o ambiente totalmente exposto a vulnerabilidades e ataques.

3.3. Do Parcelamento e Adjudicação

3.3.1. Em observância à Lei nº 14.133/2021, o objeto **não será parcelado** em lotes independentes para múltiplos fornecedores, sendo a solução agrupada em um único grupo de itens. A decisão técnica para o não parcelamento baseia-se no fato de o objeto configurar um sistema único e integrado de proteção. O parcelamento inviabilizaria a execução contratual, gerando conflitos de execução, incompatibilidade tecnológica, aumento de custos de gestão e, principalmente, lacunas na detecção correlacionada de ameaças cibernéticas avançadas

3.3.2. É expressamente **vedada a participação de empresas em consórcio**, visto a natureza avançada e altamente especializada da solução de segurança, sendo imperativo que uma única entidade seja inteiramente responsável pela coordenação técnica em todas as fases (implantação, suporte e garantia). Adicionalmente, **é vedada a subcontratação**, no todo ou em parte, do objeto. Como o serviço lida com dados críticos e estratégicos da Justiça (dados de usuários, configurações de rede, incidentes de segurança), a subcontratação introduziria riscos inaceitáveis à segurança da informação e dificultaria a apuração de responsabilidades em caso de vazamentos.

3.4. Modalidade e Tipo de Licitação

3.4.1. A modalidade de licitação a ser adotada pelo Poder Judiciário do Estado do Acre (PJAC) será o Pregão, na sua forma Eletrônica. A escolha justifica-se pelo fato de a solução de segurança cibernética enquadrar-se na categoria de bens e serviços comuns, possuindo padrões de desempenho e características técnicas usualmente encontradas e bem consolidadas no mercado de Tecnologia da Informação. O critério de julgamento será o de Menor Preço Global (Menor Preço por Grupo), nos termos da Lei nº 14.133/2021.

3.5. Critérios de Habilitação

3.5.1. Limita-se à comprovação de existência jurídica da pessoa e, quando cabível, de autorização para o exercício da atividade a ser contratada, nos termos do art. 66 da Lei nº 14.133/2021.

3.5.2. As licitantes deverão comprovar a habilitação econômico-financeira, restrita à apresentação da seguinte documentação, nos termos do art. 69 da Lei Federal n° 14.133/2021, conforme abaixo:

a. Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis do último exercício social;
b. Certidão negativa de feitos sobre falência expedida pelo distribuidor da sede da Licitante, conforme o art. 69 da Lei nº 14.133/2021.

3.5.3. As habilitações fiscal, social e trabalhista serão aferidas mediante a verificação dos seguintes requisitos, nos termos do art. 68 da Lei Federal n° 14.133/2021, conforme abaixo:

- Certidões ou atestados, regularmente emitidos pelo conselho profissional competente, quando for o caso, que demonstrem capacidade operacional na execução de serviços similares de complexidade tecnológica e operacional equivalente ou superior; A exigência de atestados será restrita às parcelas de maior relevância ou valor significativo do objeto da licitação, assim consideradas as que tenham valor individual igual ou superior a 4% (quatro por cento) do valor total estimado da contratação;
- Será admitida a exigência de atestados com quantidades mínimas de até 50% (cinquenta por cento) das parcelas de que trata o referido parágrafo, vedadas limitações de tempo e de locais específicos relativas aos atestados
- Em se tratando de serviços contínuos, o edital poderá exigir certidão ou atestado que demonstre que a Licitante tenha executado serviços similares ao objeto da licitação, em períodos sucessivos ou não, por um prazo mínimo, que não poderá ser superior a 3 (três) anos.

3.6. Critério técnico de aceitação das propostas

3.6.1. A aceitação técnica da solução XDR ofertada estará condicionada à comprovação prática e documental de que a ferramenta atende a todos os requisitos funcionais e tecnológicos estabelecidos para a proteção dos endpoints e servidores do PJAC. Poderá ser exigida, durante a fase de julgamento das propostas, a realização de uma Prova de Conceito (PoC) ou teste de bancada/homologação. Nestes testes, a licitante classificada provisoriamente em primeiro lugar deverá demonstrar, em ambiente controlado, as seguintes capacidades essenciais:

- Funcionamento integral na modalidade de serviço em nuvem (SaaS) com gerenciamento por console web centralizada.
- Detecção avançada baseada em inteligência artificial (machine learning) e análise comportamental para identificação de ameaças conhecidas e desconhecidas (como zero-day e ataques fileless).
- Capacidade efetiva de mitigação e bloqueio de ransomware, com interrupção de processos de criptografia não autorizados.
- Correlação multivetorial de eventos, integrando nativamente os alertas dos agentes instalados em estações de trabalho e servidores.
- Ações de contenção e resposta automatizada a incidentes, como o isolamento de rede do dispositivo comprometido e quarentena de arquivos maliciosos.

3.6.2. No tocante aos critérios legais e normativos, a solução de TIC e os serviços acessórios prestados pela Contratada deverão estar em estrita conformidade com:

- A Lei Geral de Proteção de Dados Pessoais (LGPD) - Lei Federal nº 13.709/2018, garantindo mecanismos tecnológicos para o resguardo, privacidade e anonimização de dados sensíveis inerentes aos processos judiciais e sistemas corporativos.
- O Marco Civil da Internet - Lei Federal nº 12.965/2014, garantindo a adequada retenção, inviolabilidade e guarda dos registros de conexão e de acesso a aplicações (logs).
- A Lei de Propriedade Intelectual de Programa de Computador (Software) - Lei Federal nº 9.609/1998.

- As diretrizes estabelecidas pela Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), consubstanciadas na Resolução CNJ nº 396/2021.
- As Políticas de Segurança da Informação (PSI) e diretrizes de governança interna expedidas pelo próprio Poder Judiciário do Estado do Acre (PJAC)..

4. DA EXECUÇÃO E GESTÃO DO CONTRATO

4.1. Papéis Desempenhados na contratação

4.1.1. Para a execução do contrato, é mandatório que os seguintes papéis e responsabilidades sejam definidos:

a) Autoridade competente: Titular da unidade/setor do órgão ou autoridade delegada, responsável pela assinatura do Contrato, Termo de compromisso de manutenção de Sigilo e pela publicação da equipe de fiscalização;
b) Gestor do Contrato: servidor com atribuições gerenciais, preferencialmente da Área Demandante da Solução de TIC (STIC), designado para coordenar e comandar o processo de gestão e fiscalização da execução contratual, indicado por autoridade competente;
c) Fiscal Técnico do Contrato: servidor representante da Área de Tecnologia da Informação e Comunicação, designado pela respectiva autoridade competente para fiscalizar o contrato quanto aos aspectos técnicos da solução;
d)Fiscal Demandante: servidor representante da Área Demandante da solução, designado pela autoridade competente dessa área para fiscalizar o contrato do ponto de vista de negócio e funcional da solução de TIC;
e) Fiscal Administrativo: servidor representante da Área Administrativa do órgão, designado pela respectiva autoridade competente para fiscalizar o contrato quanto aos aspectos administrativos da execução, especialmente os referentes ao recebimento, pagamento, sanções, aderência às normas, diretrizes, obrigações. fiscais, previdenciárias e trabalhistas e demais obrigações contratuais. O fiscal administrativo deverá ser designado pela autoridade competente e não poderá ser servidor da área de TIC, salvo em situações excepcionais, devidamente justificada, Resolução CNJ nº 468/2022, artigo 24, §3;
f) Preposto: funcionário representante da empresa Contratada, responsável por acompanhar a execução do contrato e atuar como interlocutor principal junto ao órgão contratante, incumbido de receber, diligenciar, encaminhar e responder as questões técnicas, legais e administrativas referentes ao andamento contratual; e
g) Representante da Contratada: Responsável legal da Contratada para assinatura do contrato, caso tal poder não tenha sido delegado para o preposto.

4.2. Formas de comunicação e acompanhamento da execução do contrato

4.2.1. Mecanismos formais de comunicação, entre o órgão e a Contratada a serem utilizadas para todas e quaisquer ocorrências relacionadas com o fornecimento da Solução de TIC, a exemplo:

a) Ata de Reunião;
b) Correio eletrônico (e-mail);
c) Ofício;
d) Ordem de Serviço;
e) Sistema de abertura de chamados;
f) Processo administrativo eletrônico do órgão;
g) poderão ser acrescidos outros meios de acompanhamento.

4.3. Principais marcos e eventos da Execução do contrato

4.3.1. A implantação da solução XDR respeitará um cronograma estruturado, limitando-se ao prazo máximo de 90 (noventa) dias corridos após a emissão da Ordem de Serviço, com as seguintes fases e marcos de entrega:

1. Assinatura do Contrato: Contratante e Contratada;
2. Reunião Inicial: Até o 5º dia útil após o evento 1;
3. Entrega do Plano de Implantação: Até 10 dias úteis após o evento 2;
4. Aprovação do Plano de Implantação: Até 5 dias úteis após o evento 3 (pelo PJAC);
5. Repasse de Conhecimento (Capacitação): Até 10 dias úteis após o evento 4;
6. Recebimento Provisório da Capacitação: Até 5 dias úteis após o evento 5;
7. Entrega do Software, Licenças e Suporte: Até 5 dias úteis após o evento 5;
8. Implantação da Solução: Até 20 dias úteis após o evento 5;
9. Recebimento Provisório do Software e Implantação: Até 5 dias úteis após o evento 8;
10. Recebimento Definitivo: Até 10 dias úteis após o evento 9, mediante estabilização e validação técnica da equipe do PJAC.

4.4. Dinâmica da execução

4.4.1. O local principal de orquestração do contrato será o ambiente computacional (redes e datacenters) do PJAC. Por se tratar de solução em nuvem (SaaS), a gestão será remota.

4.4.2. O contrato possuirá vigência contínua de 24 (vinte e quatro) meses, contados a partir da data de sua assinatura.

4.4.3. A prestação de serviços de implantação poderá ser executada, conforme a necessidade de não impactar os serviços jurisdicionais críticos, em horário comercial, no período noturno ou aos finais de semana. Os serviços de monitoramento, resposta a incidentes e suporte técnico corretivo funcionarão de forma ininterrupta, no regime de 24x7x365.

4.4.4. Durante a dinâmica de execução, é basilar a estrita conformidade com a Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018) e com as políticas da Estratégia Nacional de Segurança Cibernética do Poder Judiciário (Resolução CNJ nº 396/2021).

4.4.5. Capacitação necessária, quando couber, para os servidores do órgão.

4.5. Instrumentos formais de solicitação do objeto

4.5.1. O acionamento de suporte proativo/corretivo e demandas atinentes à execução das licenças e dos serviços se dará mediante Ordens de Serviço (OS), requisições registradas no Portal Web da ferramenta, e-mail dedicado, e/ou Central Telefônica (0800 ou número fixo) disponibilizados pela Contratada.

4.6. Níveis de serviço (SLA)

4.6.1. O atendimento para suporte técnico contínuo deverá obedecer rigorosamente à seguinte matriz de severidade e níveis de serviço (Acordos de Nível de Serviço - SLA), com respectivas glosas em caso de descumprimento:

- **Severidade 1 (Alta - Sistema Parado):** Exige início de atendimento técnico em até 2 horas (ou 4h presencial on-site). A restauração do serviço deve ocorrer em no máximo 8 horas. Multa (Glosa) de 10% por evento de

descumprimento.

- **Severidade 2 (Média/Alta - Alto Impacto):** Início do atendimento através de telefone/remoto em até 2 horas (ou técnico on-site em até 4h). A restauração deve ser concluída em até 16 horas. Glosa de 7,50% por evento.
- **Severidade 3 (Média - Sem impacto ao negócio):** Início de atendimento em até 6 horas. Restauração em até 24 horas. Glosa de 5%.
- **Severidade 4 (Baixa - Dúvidas e Correções Menores):** Contato em até 12 horas. Solução no mesmo dia ou próximo dia útil comercial. Glosa de 2%.

4.7. Qualificação Técnica dos Profissionais

4.7.1. Todo e qualquer serviço de Implantação, Resposta a Incidentes e Capacitação deverá, impreterivelmente, ser executado por profissionais especializados que possuam certificação técnica oficial emitida pelo fabricante da solução XDR ofertada. A referida comprovação será exigida pela equipe de fiscalização no momento da emissão da OS e/ou assinatura contratual.

4.8. Forma de recebimento provisório/definitivo e qualidade

4.8.1. O Recebimento Provisório dar-se-á, conforme os marcos estabelecidos (tópico 4.3), com a efetiva entrega dos acessos (licenças provisionadas na nuvem), entrega das documentações e o término das configurações descritas no Plano de Implantação.

4.8.2. O Recebimento Definitivo ocorrerá mediante atesto formal da Equipe de Fiscalização do Contrato, em até 10 (dez) dias úteis após o recebimento provisório, desde que o ambiente em produção tenha operado de forma estável, livre de falhas (estabilização técnica), validando-se a correlação adequada de eventos e bloqueio contra-ataques reais.

4.9. Forma de pagamento

4.9.1. O pagamento será efetuado mensalmente de forma proporcional aos serviços prestados e métricas validadas (número de licenças consumidas em Endpoints e Servidores), estando condicionado à estrita verificação do cumprimento das metas de Nível de Serviço (SLA) definidas neste instrumento.

4.9.2. Descontos originados de glosas por descumprimento de SLA serão aplicados diretamente na fatura/nota fiscal mensal, sem prejuízo da aplicação cumulativa de eventuais sanções administrativas.

4.9.3. Constitui exigência compulsória para as liquidações e pagamentos a manutenção, por parte da Contratada, de todas as condições de habilitação, exigindo-se a apresentação de Nota Fiscal acompanhada das Certidões Negativas de Débitos Trabalhistas (CNDT), regularidade do FGTS e da União, conforme a Lei nº 14.133/2021.

É vedado, em qualquer hipótese, o pagamento antecipado não justificado de forma expressa pela Administração.

4.10. Manutenção e Garantia

4.10.1. A solução gozará de garantia legal e técnica integral, com prestação de suporte especializado, pelo prazo mínimo de 24 (vinte e quatro) meses, contados sempre a partir do Termo de Recebimento Definitivo.

4.10.2. Estão abarcadas pela garantia as atualizações corretivas (resolução de bugs de sistema) e as evolutivas (novas assinaturas de inteligência, vacinas e melhorias no engine do XDR), sem quaisquer ônus adicionais para o Tribunal de Justiça do Estado do Acre.

4.11. Transferência de Conhecimento

4.11.1. A Contratada executará um serviço de Capacitação (Repasse de Conhecimento) focado nas disciplinas de Instalação, Parametrização, Threat Hunting, e Resposta a Incidentes na ferramenta XDR.

4.11.2. O curso terá carga horária mínima de 40 (quarenta) horas, destinado a 01 (uma) turma composta por servidores do PJAC. Deverão ser fornecidos laboratórios práticos com simulações de ameaças cibernéticas e fornecimento de material didático oficial do fabricante, garantindo autonomia plena ao órgão.

4.12. Direitos de Propriedade Intelectual e Direitos Autorais

4.12.1. Como a solução ofertada trata-se de um software de mercado (Comercial Off-The-Shelf), os direitos de código-fonte são de propriedade exclusiva do fabricante da solução.

4.12.2. Por outro lado, o PJAC resguarda total e exclusiva titularidade sobre os dados capturados, arquiteturas geradas, painéis de gestão criados, logs de auditoria, históricos de incidentes de segurança cibernética e todas as políticas e regras criadas no ambiente, sendo compulsória a facilitação de sua exportação ao fim do contrato.

4.13. Obrigações do Contratante

4.13.1. Disponibilizar recursos de infraestrutura tecnológica existentes (banco de dados, comunicação de rede e servidores) para a perfeita implantação dos agentes e configurações do Software as a Service (SaaS).

4.13.2. Exercer permanente acompanhamento (fiscalização administrativa e técnica), validando o cumprimento de relatórios e de SLAs de severidade e efetuando tempestivamente os pagamentos cabíveis das notas fiscais.

4.14. Obrigações da Contratada

4.14.1. O preposto e a equipe técnica assumem o compromisso legal de subscrição obrigatória do Termo de Compromisso de Manutenção de Sigilo (NDA) e Acordo de Confidencialidade de Informação.

4.14.2. Indicar formalmente equipe qualificada que manterá constante articulação com a Fiscalização de TI do Tribunal. A empresa deve, num prazo não superior a 24 horas, afastar qualquer profissional cujo comportamento prejudique a segurança e as rotinas do PJAC.

4.14.3. Não poderá haver, em hipótese alguma, subcontratação do serviço, sob pena de rescisão e multas, visando limitar a exposição dos dados sensíveis do Tribunal.

4.14.4. Responder irrestritamente por perdas e danos materiais ocorridos em relação aos ativos computacionais, sistemas operacionais ou dados do TJAC causados por imprudência, negligência ou falhas de configuração executadas por sua equipe durante as atividades de implantação e operação.

4.15. Estimativa de preços

4.15.1. O valor referencial global estimado para a execução desta contratação é de 1.269.927,23 (um milhão, duzentos e sessenta e nove mil, novecentos e vinte e sete reais e vinte e três centavos), consubstanciado na precificação das

licenças para endpoint, servidores e pacote de serviços de implantação, suporte e capacitação estipulados no Estudo Técnico Preliminar.

4.16. Adequação orçamentária

4.16.1. As despesas demandadas pelo custeio deste termo onerarão a dotação orçamentária respectiva ao Aprimoramento da Segurança Cibernética, enquadradas no:

- **Programa de Trabalho:** 203.617.02.061.2293.2296.0000;
- **Fonte de Recursos:** 1.760.0700; e
- **Elemento de Despesa:** 3.3.90.40.21 (Serviços de Segurança da Informação).

4.17. Reajustamento

4.17.1. Como a presente contratação engloba soluções na qual não incide o regime de dedicação exclusiva de mão de obra, os preços pactuados ficarão sujeitos a reajustamento em sentido estrito após o interregno mínimo de 1 (um) ano, aplicando-se indexadores de variação dos custos da Tecnologia da Informação (ex: IPCA/IBGE ou ICTI/Governo Federal), de modo a reequilibrar o contrato no transcurso temporal de sua vigência original de 24 meses.

4.18. Sanções Administrativas

4.18.1. Com fundamento no capítulo I do título IV da Lei Federal n° 14.113/2021, a Contratada ficará sujeita às sanções previstas em contrato no caso de descumprimento das obrigações pactuadas, sem prejuízo das responsabilidades civil e criminal, e assegurada a prévia e ampla defesa.

4.18.2. As sanções administrativas a seguir poderão ser aplicadas cumulativamente.

4.18.3. A Licitante ou a Contratada será responsabilizado administrativamente pelas seguintes infrações:

I. dar causa à inexecução parcial do contrato;
II. dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;
III. dar causa à inexecução total do contrato;
IV. deixar de entregar a documentação exigida para o certame;
V. não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;
VI. não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;
VII. ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;
VIII. apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação ou a execução do contrato;
IX. fraudar a licitação ou praticar ato fraudulento na execução do contrato;
X. comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;
XI. praticar atos ilícitos com vistas a frustrar os objetivos da licitação;
XII. praticar ato lesivo previsto no art. 5º da Lei Federal n° 12.846/2013.

4.18.4. Serão aplicadas ao responsável pelas infrações administrativas previstas na Lei Federal nº 14.133/2021 as seguintes sanções:

a) advertência;
b) multa;
c) impedimento de licitar e contratar;
d) declaração de inidoneidade para licitar ou contratar.

4.18.5. Na aplicação das sanções serão considerados:

1. a natureza e a gravidade da infração cometida;
2. as peculiaridades do caso concreto;
3. as circunstâncias agravantes ou atenuantes;
4. os danos que dela provierem para a Administração Pública;
5. a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

4.18.6. A sanção prevista no item 4.18.4 será aplicada exclusivamente pela infração administrativa prevista no inciso I do item 4.18.3, quando não se justificar a imposição de penalidade mais grave.

4.18.7. A sanção prevista na alínea "b" do item 4.18.4, calculada na forma do edital ou do contrato, não poderá ser inferior a 0,5% (cinco décimos por cento) nem superior a 30% (trinta por cento) do valor do contrato licitado ou celebrado com contratação direta e será aplicada ao responsável por qualquer das infrações administrativas previstas no 4.18.3.

4.18.8. A sanção prevista na alínea "c" do item 4.18.4 será aplicada ao responsável pelas infrações administrativas previstas nos incisos II, III, IV, V, VI e VII do item 4.18.3, quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta do ente federativo que tiver aplicado a sanção, pelo prazo máximo de 3 (três) anos.

4.18.9. A sanção prevista na línea "d" do item 4.18.4 será aplicada ao responsável pelas infrações administrativas previstas nos incisos VIII, IX, X, XI e XII do item 4.18.3, bem como pelas infrações administrativas previstas nos incisos II, III, IV, V, VI e VII que justifiquem a imposição de penalidade mais grave que a sanção referida no item 4.18.8, e impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos.

4.18.10. A sanção estabelecida na alínea "d" do item 4.18.4 será precedida de análise jurídica, desde que observada, quando aplicada por órgãos dos Poderes Legislativo e Judiciário, pelo Ministério Público e pela Defensoria Pública no desempenho da função administrativa, será de competência exclusiva de autoridade de nível hierárquico equivalente autoridade máxima da entidade.

4.18.11. As sanções previstas nas alíneas "a", "c" e "d" do item 4.18.4 poderão ser aplicadas cumulativamente com a prevista na alínea ‘b" do mesmo item.

4.18.12. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor de pagamento eventualmente devido pelo Poder Judiciário do Estado do Acre aa Contratada, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente.

4.18.13. A aplicação das sanções previstas neste tópico não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado à Administração Pública.

4.18.14. Na aplicação da sanção prevista na alínea "b" do item 4.18.4, será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação.

4.18.15. A aplicação das sanções previstas nas alíneas "c" e "d" do item 4.18.4 requererá a instauração de processo de responsabilização, a ser conduzido por comissão composta de 2 (dois) ou mais servidores estáveis, que avaliará fatos e

circunstâncias conhecidos e intimará a Licitante ou a Contratada para, no prazo de 15 (quinze) dias úteis, contado da data de intimação, apresentar defesa escrita e especificar as provas que pretenda produzir.

4.18.16. O atraso injustificado na execução do contrato sujeitará a Contratada a multa de mora, na forma prevista em edital ou em contrato.

4.18.17. A aplicação de multa de mora não impedirá que o Poder Judiciário do Estado do Acre converta em compensatória e promova a extinção unilateral do contrato com a aplicação cumulada de outras sanções previstas na Lei Federal n° 14.133/2021.

5. REQUISITOS TÉCNICOS

5.1. Aspectos Funcionais da Solução

5.1.1. Proteção Multivetorial e Detecção Baseada em Comportamento:

A plataforma de proteção de endpoints (EPP) e de detecção e resposta estendida (XDR) deverá possuir uma abordagem técnica proativa focada em ameaças conhecidas e desconhecidas.

O engine de detecção deve incorporar algoritmos de Machine Learning tanto em fase de pré-execução quanto em runtime, garantindo a mitigação de técnicas de ofuscação de código e ataques fileless executados diretamente em memória (RAM).

A solução deve bloquear de forma autônoma processos característicos de ataques de ransomware e possuir a capacidade técnica de interrupção imediata da rotina de criptografia, executando o rollback e restaurando os arquivos originais aos seus respectivos diretórios.

A proteção de memória deve atuar contra exploits que utilizem técnicas de injeção de código e buffer overflow.

5.1.2. Módulos do Agente para Estações de Trabalho (Endpoints):

O agente unificado para estações deverá ser plenamente compatível com os sistemas operacionais Windows (8.1, 10, 11) e macOS. O sensor deverá consolidar os seguintes vetores de defesa técnica:

- Anti-Malware e Heurística Avançada: Inspeção profunda de processos, interceptação de chamadas de sistema, e capacidade de varredura recursiva em arquivos compactados em até 6 níveis de compressão e 20 níveis para arquivos OLE, realizando a neutralização exclusiva do artefato malicioso sem comprometer o arquivo consolidado. Integração com interface AMSI (Antimalware Scan Interface) para sistemas Windows.
- Host IPS (HIPS) e Host Firewall: Inspeção de tráfego stateful bidirecional no host, capacidade de detecção de Network Scan e Port Scan com bloqueio temporário dinâmico, e controle granular sobre a pilha TCP/UDP com suporte a regras por direção, endereço MAC, cabeçalhos, e restrições de limite de conexões para prevenir ACK storms.
- Controle de Aplicações (Application Control): Capacidade de restringir execuções baseadas em assinaturas de hash (SHA-1 e SHA-256), cadeia de certificados digitais e caminhos lógicos.
- Controle Granular de Dispositivos (Device Control): Gerenciamento rigoroso de mídias de armazenamento USB, bloqueio de execuções automáticas (Autorun), e capacidade de filtrar interfaces infravermelhas, Bluetooth e portas COM/LPT.

5.1.3. Módulos Avançados para Cargas de Trabalho (Servidores):

A proteção de servidores deverá suportar matrizes heterogêneas amplas, incluindo instâncias Windows Server (2000 a 2022), distribuições Linux (Red Hat, CentOS, Debian, Ubuntu, Suse), variantes Unix (AIX, Solaris, HP-UX) e hipervisores VMware. Para tais cargas de trabalho, exigem-se os seguintes módulos:

- Inspeção Profunda e Virtual Patching: Implantação autônoma de regras de Intrusion Detection/Prevention Systems (IDS/IPS) baseadas no inventário das vulnerabilidades do SO e das aplicações instaladas, viabilizando o bloqueio de SQL Injection, Cross-Site Scripting (XSS) e outras explorações catalogadas em CVEs.
- Monitoramento de Integridade de Arquivos (FIM): Identificação contínua, com acionamento pseudo real-time no Linux e real-time no Windows, de alterações de estado em diretórios críticos, daemons, portas de comunicação e chaves de registro do sistema.
- Inspeção Dinâmica de Logs: Coleta, extração sistemática de indicadores de comprometimento (IoCs) e correlação de eventos gerados por serviços e aplicações de terceiros (ex: IIS, Apache, Bancos de Dados) e do sistema operacional.

5.1.4. Telemetria e Resposta a Incidentes (EDR/XDR):

O mecanismo de rastreio deverá mapear ativamente todos os alertas em táticas e técnicas definidas no framework MITRE ATT&CK®. A correlação de eventos deve ser nativa, integrando dados de endpoints, servidores e rede diretamente na nuvem do fabricante. A equipe de segurança deverá conseguir orquestrar ações remotas avançadas, incluindo: isolamento cibernético do host (mantendo a conectividade restrita com a console de gerência), coleta remota de arquivos (download do artefato), interrupção arbitrária de processos da árvore de execução, e estabelecimento de terminal seguro (Remote Shell) para comandos forenses no equipamento isolado. Os dados de telemetria bruta para threat hunting deverão possuir retenção contínua mínima de 30 (trinta) dias.

5.2. Arquitetura Tecnológica

5.2.1. Plataforma em Nuvem (SaaS):

A arquitetura base do sistema central deverá ser entregue na modalidade Software as a Service gerida integralmente pelo fabricante, suportando Alta Disponibilidade, dashboards customizáveis por usuário e integração por API aberta baseada em cookbooks para inserção da solução em esteiras automatizadas de DevSecOps e orquestração.

5.2.2. Interoperabilidade e Governança:

O sistema deverá suportar conexões fluídas e nativas com plataformas de nuvem (AWS, Azure, vCloud). É exigida compatibilidade protocolar para direcionamento sistemático dos logs capturados aos servidores Syslog e plataformas SIEM da infraestrutura existente (ex: Splunk, IBM QRadar, HP ArcSight).

A ferramenta deverá utilizar federação de identidades baseada em SAML ou protocolo equivalente (Single Sign-On), integrando-se nativamente com Active Directory com suporte a múltiplas florestas de domínios.

5.2.3. Criptografia e Gerência de Banda:

As conexões bidirecionais firmadas entre os agentes finais e a console em nuvem do fabricante deverão ocorrer de modo criptografado usando TLS/SSL, possuindo cada agente a sua respectiva e exclusiva chave criptográfica. A solução deve possuir a capacidade de designar instâncias específicas como "Agentes Replicadores", que atuam no cacheamento incremental e distribuição interna local das vacinas e políticas para evitar saturação excessiva dos links WAN do Tribunal.

5.3. Projeto e Implementação

5.3.1. Planejamento Tático: O cronograma do projeto e a implantação não devem ultrapassar 90 (noventa) dias após o recebimento da Ordem de Serviço, seguindo fases rígidas que englobam o planejamento, configuração de ambiente, testes em sub-redes (piloto/homologação), e o rollout em massa com desinstalação técnica automatizada. O fornecedor apresentará um Plano de Implantação estipulando matrizes de riscos, topologia L2/L3 e cronogramas lógicos pormenorizados.

5.3.2. Mecanismos de Instalação Massiva:

A implementação (deploy) deve ser compatível com ferramentas corporativas de mercado, como Microsoft System Center Configuration Manager (SCCM), Puppet, ou métodos similares.

A execução da instalação exigirá formato de pacotes do tipo MSI (ativados de forma automatizada por scripts PowerShell) em plataformas Windows, e formatos DEB/RPM controlados via bash scripts nas plataformas baseadas em núcleo Linux.

A instalação requer a característica silent install, bem como a desinstalação automática, silenciosa e remota da solução predecessora (antivírus legado), sem necessidade de plugins ou softwares acessórios para esta operação de saneamento do sistema operacional.

5.4. Manutenção, Atualizações e Garantia Contratual

5.4.1. O período técnico e vinculativo da garantia, durante o qual todas as funcionalidades, assinaturas de ameaças e correções de bugs de sistema estarão acobertadas, será de 24 (vinte e quatro) meses, tendo início formal unicamente na data de assinatura do Termo de Recebimento Definitivo.

5.4.2. Durante a vigência total, o ciclo de vida do software exige updates automáticos, evoluções de engine e vacinas liberadas de modo autônomo e agendado pelo sistema. Suporte técnico e serviço corretivo/preventivo ininterrupto (24x7x365) atuarão sob diretrizes rigorosas baseadas em Severidade Crítica, nas quais paradas totais (Severidade 1) impõem um Service Level Agreement (SLA) de restauração do serviço e entrega da solução técnica contornável no prazo máximo de 8 (oito) horas sob pena de aplicação mandatória de glosa técnica de 10% do faturamento.Todo o corpo funcional alocado pela Contratada neste serviço de implantação, administração técnica de console e troubleshooting avançado deverá possuir, inequivocamente, certificação especializada outorgada pelo fabricante oficial da solução XDR ofertada.

5.5. Procedimentos Técnicos de Avaliação, Testes e Recebimento

5.5.1. A conformidade será chancelada e a aprovação sujeitar-se-á aos trâmites do art. 140 da Lei nº 14.133/2021 e do art. 19 da Instrução Normativa SGD/ME nº 94/2022, cabendo à Equipe de Fiscalização a chancela mediante evidências

objetivas exaradas por listas de verificação, monitoramentos no painel gerencial da solução, inspeções in loco (ou avaliações remotas da estrutura lógica hospedada) e validação técnica da integração contínua.

5.5.2. Teste de Bancada / Prova de Conceito (PoC):

Em atenção aos preceitos da avaliação de qualidade funcional da tecnologia pretendida, o Tribunal detém a prerrogativa de exigir da Contratada (ou licitante mais bem qualificada), em ambiente rigorosamente segregado do barramento de produção, simulações técnicas consubstanciadas no escopo do edital. Os roteiros de execução da PoC contemplarão as verificações da interrupção forçada de ataques fileless, demonstração empírica da neutralização e restauração de diretórios acometidos por técnicas simuladas de ransomware (funcionalidade de rollback), orquestração da integração SAML/SSO com as bases legadas, isolamento remoto de estações contagiadas, e as devidas demonstrações da análise heurística da solução ofertada.

6. ASSINATURAS

Em atendimento ao art. 12, § 6º da Instrução Normativa SGD/ME nº 94, de 2022, a Equipe de Planejamento da Contratação, instituída pela Portaria nº 3847/2025, de 20 de Agosto de 2025, bem como pela autoridade competente da área de TIC, assinam o Termo de Referência, atestando sua conformidade às disposições da Resolução CNJ nº 468/2022.

7. APROVAÇÃO

Em atendimento ao art. 12, § 6º da Instrução Normativa SGD/ME nº 94, de 2022, a autoridade competente do Órgão aprova o Termo de Referência, atestando sua conformidade às disposições da Resolução CNJ nº 468/2022.

Assinatura Eletrônica da Comissão Permanente de Contratações de Tecnologia da Informação e Comunicação:

Amilar Sales Alves
Subsecretário de Segurança da Informação
Integrante Demandante - Portaria nº 3847/2025/TJAC

Eliélcio Canedo da Silva
Subsecretário de Contratações de TIC
Integrante Técnico - Portaria nº 3847/2025/TJAC

Ângelo Máximo de Melo Silva
Chefe da Divisão de Contratações de TIC
Integrante Técnico - Portaria nº 3847/2025/TJAC

Allexandra Macedo de Souza Oliveira
Equipe de Apoio

PODER JUDICIÁRIO
DO ESTADO DO ACRE

Integrante Administrativo - Portaria nº 3847/2025/TJAC

Documento assinado eletronicamente por **ANGELO MAXIMO DE MELO SILVA**, em 15/05/2026 às 12:09:29.

Documento assinado eletronicamente por **ELIELCIO CANEDO DA SILVA**, **Técnico Judiciário** em 15/05/2026 às 11:50:46.

Para conferir a autenticidade do documento, utilize um leitor de QRCode ou acesse o endereço **http://appgrp.tjac.jus.br/grp/acessoexterno/programaAcessoExterno.faces?codigo=670270** e informe a chancela **3LS7.TFGZ.WYGR.ODBY**