PODER JUDICIÁRIO
DO ESTADO DO ACRE

ESTUDO TÉCNICO PRELIMINAR (TIC) Nº 5/2025

Processo Administrativo nº 319/2025

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, 10 de Julho de 2025.

PODER JUDICIÁRIO
DO ESTADO DO ACRE

ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO

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

1. ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO

1.1. Contextualização

O Poder Judiciário do Estado do Acre (PJAC) necessita adquirir uma solução moderna e integrada de segurança para endpoints, com foco específico na proteção de estações de trabalho e servidores, como medida estratégica para garantir a continuidade, confiabilidade e segurança dos serviços jurisdicionais prestados à sociedade. A contratação de uma solução de Detecção e Resposta Estendida (XDR – Extended Detection and Response) tem como finalidade fortalecer a capacidade institucional de prevenção, detecção e resposta a incidentes cibernéticos que impactam diretamente as atividades finalísticas do Tribunal.

O parque tecnológico do PJAC é composto por aproximadamente 2.700 equipamentos, entre máquinas clientes e servidores, atendendo cerca de 2.100 usuários ativos, incluindo magistrados, servidores e colaboradores. Esse ambiente sustenta sistemas judiciais eletrônicos, serviços administrativos, canais digitais de atendimento ao cidadão, audiências virtuais e fluxos processuais essenciais à prestação jurisdicional. A indisponibilidade, comprometimento ou degradação desses recursos tecnológicos afeta diretamente o direito fundamental de acesso à Justiça, causando prejuízos ao jurisdicionado e à sociedade.

Atualmente, o PJAC utiliza uma solução antivírus tradicional, baseada exclusivamente em assinaturas de ameaças conhecidas, que não acompanha a evolução do cenário de ameaças cibernéticas. Além de não atender mais ao quantitativo atual de equipamentos, essa solução possui limitações técnicas relevantes, como ausência de análise comportamental, correlação de eventos, resposta automatizada e visibilidade contextual. Trata-se de uma abordagem reativa, incapaz de identificar ataques sofisticados, como ameaças de dia zero, ransomware avançado, movimentação lateral e uso indevido de credenciais legítimas.

O cenário nacional demonstra um aumento significativo de ataques direcionados aos endpoints do Poder Judiciário, uma vez que esses dispositivos representam o principal ponto de entrada para comprometimento de sistemas críticos. Esse contexto é reconhecido pelo Conselho Nacional de Justiça, por meio da Resolução CNJ nº 396/2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário, exigindo dos tribunais a adoção de mecanismos eficazes de detecção, resposta e gestão de incidentes. Soma-se a isso as novas diretrizes de segurança cibernética e proteção de dados publicadas pelo STF em 2024, que reforçam a necessidade de gestão de riscos, monitoramento contínuo, controle de acessos e resposta estruturada a incidentes, em consonância com a LGPD.

Nesse contexto, o XDR (Extended Detection and Response) se apresenta como tecnologia essencial para o PJAC. Trata-se de uma abordagem avançada de segurança que correlaciona dados provenientes dos endpoints e de outras camadas de segurança, permitindo identificar comportamentos anômalos, investigar cadeias de ataque e executar respostas automáticas ou orquestradas em tempo real. Diferentemente de soluções antivírus convencionais, o XDR analisa o ambiente como um todo, utilizando inteligência analítica, aprendizado de máquina e contexto operacional para reduzir o tempo de exposição a ameaças e minimizar impactos operacionais.

A adoção dessa solução proporciona benefícios diretos ao negócio do PJAC, tais como:

- Redução do risco de indisponibilidade dos sistemas judiciais, assegurando a continuidade da prestação jurisdicional;
- Proteção de dados sensíveis de processos judiciais e informações pessoais de cidadãos, em conformidade com a LGPD;
- Mitigação de incidentes que possam atrasar prazos processuais, audiências e decisões judiciais;
- Aumento da confiança do jurisdicionado nos serviços digitais do Tribunal, fortalecendo a imagem institucional;
- Maior eficiência operacional da área de TIC, com redução de incidentes recorrentes e respostas mais rápidas.

É importante ressaltar que esta contratação possui escopo específico e delimitado à proteção de endpoints (máquinas clientes e servidores), não se confundindo com futuras contratações de SOC, NDR, UEBA e outras. O XDR representa uma camada técnica fundamental e prévia, responsável por detectar e conter ameaças diretamente nos dispositivos utilizados pela instituição. Caracteriza-se como solução especializada de segurança para endpoints, com capacidade de detecção avançada, resposta automatizada e análise contextual de riscos, permitindo ao PJAC reduzir sua superfície de ataque.

Adicionalmente, a solução pretendida deverá ser integrável às demais camadas de segurança existentes, permitindo uma arquitetura de defesa em profundidade e fornecendo subsídios técnicos para análises de risco contínuas, tanto operacionais quanto gerenciais.

Dessa forma, a aquisição de uma solução de XDR robusta, escalável e interoperável é essencial para atender às necessidades de negócio do PJAC, proteger os ativos de informação institucionais e garantir que o cidadão acreano continue tendo acesso seguro, confiável e ininterrupto aos serviços judiciais, mesmo diante do crescimento e da sofisticação das ameaças cibernéticas.

1.2. Identificação da demanda no Plano de Contratações de STIC

A demanda pela solução XDR para endpoint encontra-se plenamente alinhada e prevista no Plano de Contratações de Soluções de Tecnologia da Informação e Comunicação (PSTIC/2026) do Poder Judiciário do Estado do Acre, conforme as diretrizes do planejamento estratégico da Administração.

1.2.1. Alinhamento da Solução

Plano Estratégico Institucional: PEI: Perspectiva do Aprendizado e Crescimento.
Macrodesafio: Fortalecer a Gestão de TIC.
Objetivo: Definir e executar projetos estratégicos de TIC no TJ, conforme resoluções do CNJ.
Meta: Modernizar a estrutura de TI em 70% até 2026.

Plano Diretor institucional (PDTIC): O PDTIC é um instrumento que visa direcionar os investimentos e aquisições de bens e serviços de TIC, objetivando maximizar o cumprimento da estratégia institucional 2021/2026, em consonância às normas nacionais do Poder Judiciário e à visão de longo prazo do Tribunal de Justiça do Acre.

Plano de Contratação de Soluções de Tecnologia da Informação Comunicação - PSTIC: A contratação ora pleiteada está prevista no Plano Anual de Contratação de TIC 2026.

1.3. Caracterização da demanda

1.3.1. Definição e Especificação das Necessidades

O Poder Judiciário do Estado do Acre (PJAC) necessita fortalecer a segurança de seu ambiente computacional por meio da adoção de uma solução avançada de proteção de endpoints, abrangendo estações de trabalho e servidores que sustentam os sistemas judiciais, administrativos e os serviços digitais disponibilizados à sociedade.

Identifica-se a necessidade de uma solução especializada que possibilite a detecção avançada de ameaças, resposta rápida a incidentes de segurança e análise contínua de riscos nos endpoints, considerando o volume e a criticidade dos ativos tecnológicos do PJAC. Tal necessidade decorre da crescente sofisticação das ameaças cibernéticas e do papel essencial da infraestrutura de TI na garantia da disponibilidade, integridade e confidencialidade das informações judiciais.

A adoção da solução visa diminuir a superfície de ataque com o intuito de garantir a continuidade dos serviços jurisdicionais, minimizar riscos de indisponibilidade de sistemas, vazamento de dados ou comprometimento de informações sensíveis, impactando diretamente o jurisdicionado e o cidadão atendido pelo TJAC, que dependem de serviços digitais confiáveis, estáveis e seguros para o exercício de seus direitos.

1.3.2. Definição e Especificação de Requisitos

A solução a ser contratada deverá atender aos requisitos técnicos necessários para a proteção eficaz dos endpoints do PJAC, considerando o porte do ambiente, a criticidade dos serviços suportados e as diretrizes normativas aplicáveis ao Poder Judiciário.

A solução deverá ser classificada como XDR (Extended Detection and Response), com foco específico em máquinas clientes e servidores, possibilitando monitoramento contínuo, análise comportamental e correlação de eventos de segurança. Deverá permitir respostas automáticas ou orquestradas a incidentes, bem como análise de risco baseada em contexto, priorizando ativos e eventos conforme seu impacto potencial.

Deverá ser escalável, compatível com o crescimento do parque computacional e integrável às demais camadas de segurança existentes ou futuras, observando as boas práticas de segurança da informação e a conformidade com a legislação vigente.

1.3.3. Requisitos Funcionais

A solução deverá prover proteção contínua para estações de trabalho e servidores do PJAC, com monitoramento em tempo real e análise de eventos de segurança.

Deverá detectar ameaças conhecidas e desconhecidas por meio de análise comportamental, heurística avançada e correlação de eventos, não se limitando a assinaturas tradicionais.

A solução deverá identificar e mitigar ataques como ransomware, ameaças de dia zero, ataques fileless, movimentação lateral e uso indevido de credenciais.

Deverá permitir respostas automáticas ou assistidas, incluindo isolamento de dispositivos, bloqueio de processos maliciosos e quarentena de arquivos suspeitos.

Deverá disponibilizar visibilidade dos incidentes com linha do tempo dos eventos e geração de relatórios técnicos e gerenciais.

Deverá possibilitar aplicação granular de políticas de segurança e administração centralizada com controle de acesso por perfis.

Os requisitos estabelecidos consideram as boas práticas de segurança da informação e a criticidade dos serviços judiciais suportados pelo PJAC.

SOLUÇÃO DE PROTEÇÃO DE ENDPOINTS COM ABORDAGEM PROATIVA PARA RESPOSTA EFICAZ A INCIDENTES

Características gerais

A solução deverá ser entregue na modalidade como um serviço (em nuvem);

Possuir console Web para gerenciamento e administração da ferramenta;

A proteção para estações de trabalho deverá prover Anti-Malware, Firewall, Host IPS, Controle de Aplicações e Controle de dispositivos em um único agente.

Módulo de Proteção Anti-Malware

Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:

- Windows 8.1 (x86/x64);
- Windows 10 (x86/x64);
- Windows 11 (x64).

Deve disponibilizar evidências de varredura em todas as estações de trabalho, identificando as atualizações de sucesso e as ações de insucesso, para garantir que os casos de insucesso sejam monitorados para tomada de ações pontuais;

Deve detectar, analisar e eliminar programas maliciosos, tais como vírus, spyware, worms, cavalos de tróia, keyloggers, programas de propaganda, rootkits, phishing, dentre outros;

Deve detectar, analisar e eliminar, automaticamente e em tempo real, programas maliciosos em: Processos em execução em memória principal (RAM);

Arquivos executados, criados, copiados, renomeados, movidos ou modificados, inclusive em sessões de linha de comando (DOS ou Shell).

Deve escanear arquivos compactados automaticamente, em pelo menos nos seguintes formatos: zip, exe, arj, MIME/uu, CAB;

Deve escanear arquivos recebidos por meio de programas de comunicação instantânea (MSN messenger, yahoo messenger, google talk, icq, dentre outros);

Deve detectar e proteger em tempo real a estação de trabalho contra vulnerabilidades e ações maliciosas executadas em navegadores web por meio de scripts em linguagens tais como Javascript, VBScript/Activex;

Deve possuir detecção heurística de vírus desconhecidos;

Deve permitir configurar o consumo de CPU que será utilizada para uma varredura manual ou agendada;

Deve permitir diferentes configurações de detecção (varredura ou rastreamento):

Em tempo real de arquivos acessados pelo usuário;

Em tempo real dos processos em memória, para a captura de programas maliciosos executados em memória, sem a necessidade de escrita de arquivo;

Manual, imediato ou programável, com interface gráfica em janelas, personalizável, com opção de limpeza;

Automáticos do sistema com as seguintes opções:

Escopo: todos os discos locais, discos específicos, pastas específicas ou arquivos específicos;

Ação: somente alertas, limpar automaticamente, apagar automaticamente, renomear automaticamente, ou mover automaticamente para área de segurança (quarentena);

Frequência: horária, diária, semanal e mensal;

Exclusões: pastas ou arquivos (por nome e/ou extensão) que não devem ser rastreados.

Deve possuir mecanismo de cache de informações dos arquivos já escaneados;

Deve possuir cache persistente dos arquivos já escaneados para que, nos eventos de desligamento e reinicialização das estações de trabalho e notebooks, a cache não seja descartada;

Deve possuir ferramenta de alterações de parâmetros de comunicação entre o cliente antivírus e o servidor de gerenciamento da solução de antivírus;

Deve permitir a utilização de servidores locais de reputação para análise de arquivos e URL's maliciosas, de modo a prover rápida detecção de novas ameaças;

Deve ser capaz de aferir a reputação das URL's acessadas pelas estações de trabalho e notebooks, sem a necessidade de utilização de qualquer tipo de programa adicional ou plug-in ao navegador web, de forma a proteger o usuário independentemente da maneira de como a URL está sendo acessada;

Deve ser capaz de detectar variantes de malwares que possam ser geradas em tempo real na memória da estação de trabalho ou notebook, permitindo que seja tomada ação de quarentena a ameaça;

Deve possuir capacidade de escaneamento de arquivos compactados e, em caso de identificação de um arquivo malicioso, apenas este deve ser removido, mantendo os demais intactos;

Deve ser capaz de bloquear o acesso a qualquer site não previamente analisado pelo fabricante;

Deve permitir a restauração de maneira granular de arquivos quarentenados sob suspeita de representarem risco de segurança;

Deve permitir, em conjunto com a restauração dos arquivos quarentenados, a adição automática às listas de exclusão de modo a evitar novas detecções dos arquivos;

Deverá ter funcionalidade de Machine Learning para detectar e tomar ações sobre ameaças desconhecidas e suspeitas;

Deverá ter funcionalidade de Machine Learning em runtime para evitar possíveis métodos de obfuscação que o módulo de Machine Learning em pré-execução não consiga detectar;

Deve fornecer um informativo compreensivo de cada simulação que descreva as ações e respectivos metadados, bem como o porquê do veredito emitido pela Machine Learning;

Deve bloquear processos comuns associados a ransomware;

Em casos de ataques de ransomware, a solução deve ter a capacidade de interromper o processo de criptografia e restaurar os arquivos originais aos seus respectivos diretórios;

Deve possuir funcionalidade de detecção de malwares conhecidos e desconhecidos por comportamento;

Deve permitir a integração com solução de análise de artefatos suspeitos (sandbox) do próprio fabricante.

Funcionalidade de Atualização

Deve permitir a programação de atualizações automáticas das listas de definições de vírus, a partir de local predefinido da rede, ou de site seguro da internet, com frequência (no mínimo diária) e horários definidos pelo administrador da solução;

Deve permitir atualização incremental da lista de definições de vírus;

Deve permitir a atualização automática do engine do programa de proteção a partir de localização na rede local ou na internet, a partir de fonte autenticável;

Deve permitir o rollback das atualizações das listas de definições de vírus e engines;

Deve permitir a indicação de agentes para efetuar a função de replicador de atualizações e configurações, de forma que outros agentes possam utilizá-los como fonte de atualizações e configurações, não sendo necessária a comunicação direta com o servidor de anti-malware para essas tarefas;

Deve permitir que os agentes de atualização possam replicar os componentes de vacinas, motores de escaneamento, versão de programas, hotfix e configurações específicas de domínios da árvore de gerenciamento;

O agente replicador de atualizações e configurações deve ser capaz de gerar localmente versões incrementais das vacinas a serem replicadas com os demais agentes locais, de maneira a reduzir o consumo de banda necessário para execução da tarefa de atualização.

Funcionalidade de Administração

Deve permitir proteção das configurações da solução instalada na estação de trabalho através de senha ou controle de acesso, em ambos os casos, controlada por política gerenciada pela console de administração da solução completa;

Deve possibilitar instalação “silenciosa”;

Deve permitir o bloqueio por nome de arquivo;

Deve permitir o travamento de pastas e diretórios;

Deve permitir o travamento de compartilhamentos;

Deve permitir o rastreamento e bloqueio de infecções;

Deve possuir mecanismo de detecção de ameaças baseado em comportamento de processos que estão sendo executados nas estações de trabalho e notebooks;

Deve desinstalar automática e remotamente a solução de antivírus atual, sem requerer outro software ou agente;

Deve permitir a desinstalação através da console de gerenciamento da solução;

Deve ter a possibilidade de exportar/importar configurações da solução através da console de gerenciamento;

Deve permitir a deleção dos arquivos quarentenados;

Deve permitir remoção automática de clientes inativos por determinado período;

Deve permitir integração com serviço de autenticação como Active Directory para acesso à console de administração;

Deve permitir criação de diversos perfis e usuários para acesso à console de administração;

Deve permitir que a solução utilize consulta externa a base de reputação de sites integrada e gerenciada através da solução de anti-malware, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;

Deve possuir solução de consulta do hash dos arquivos integrada e gerenciada através da solução de antivírus, cancelando o download ou execução do arquivo, de forma automática, baseado na resposta à consulta da base do fabricante;

Deve permitir criação de subdomínios consecutivos dentro da árvore de gerenciamento;

Deve possuir solução de reputação de sites local para sites já conhecidos como maliciosos integrada e gerenciada através da solução de antivírus, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;

Deve registrar no sistema de monitoração de eventos da console de anti-malware informações relativas ao usuário logado no sistema operacional;

Deve prover ao administrador relatório de conformidade do status dos componentes, serviços e configurações das estações de trabalho e notebooks que fazem parte do escopo de gerenciamento da console;

Deve prover criptografia para as comunicações entre o servidor e os agentes de proteção;

Deve suportar múltiplas florestas e domínios confiáveis do Active Directory;

Deve utilizar de chave de criptografia que seja/esteja em conformidade com o Active Directory para realizar uma conexão segura entre servidor e controlador de domínio;

Deve permitir a criação de usuários locais de administração da console de anti-malware;

Deve possuir integração com o Active Directory para utilização de seus usuários para administração da console;

Deve permitir criação de diversos perfis de usuários que permitam acessos diferenciados e customizados a diferentes partes da console de gerenciamento;

Deve se utilizar de mecanismo de autenticação da comunicação entre o servidor de administração e os agentes de proteção distribuídos nas estações de trabalho e notebooks;

Deve permitir a gerência de domínios separados para usuários previamente definidos;

Deve ser capaz de enviar notificações específicas aos respectivos administradores de cada domínio definido na console de administração;

Deve permitir configuração do serviço de reputação de sites da web em níveis: baixo, médio e alto.

Funcionalidade de Controle de Dispositivos

As configurações da funcionalidade de controle de dispositivos devem ser aplicadas por usuário;

Deve permitir políticas e ações diferentes para dispositivos conectados à rede interna e aqueles utilizados na rede externa (conectado à Internet, por exemplo);

Deve possuir controle de acesso a discos removíveis reconhecidos como dispositivos de armazenamento em massa através de interfaces USB e outras, com as seguintes opções: acesso total, leitura e escrita, leitura e execução, apenas leitura e bloqueio total;

Deve possuir o controle de acesso a drives de mídias de armazenamento como CD-ROM, DVD, com as opções de acesso total, leitura e escrita, leitura e execução, apenas leitura e bloqueio total;

Deve ser capaz de identificar smartphones e tablets como destinos de cópias de arquivos e tomar ações de controle da transmissão;

Deve possuir o controle a drives mapeados com as seguintes opções: acesso total, leitura e escrita, leitura e execução, apenas leitura e bloqueio total;

Deve permitir escaneamento dos dispositivos removíveis e periféricos (USB, disquete, cdrom) mesmo com a política de bloqueio total ativa;

Para ação de restrição como o bloqueio, a solução deve permitir adicionar dispositivos USB autorizados, bem como apontar executáveis específicos como exceção ao bloqueio;

Deve ter a capacidade de bloquear a função de Autorun nos dispositivos;

Deve permitir controle de permissão ou bloqueio para dispositivos que não armazenam dados tendo, pelo menos, os seguintes tipos de dispositivos: adaptadores bluetooth, dispositivos de imagem, modems, interfaces wireless externas, cartões PCMCIA, dispositivos infravermelhos e portas COM/LPT.

Módulo de Proteção Anti-Malware para estações MacOS

O cliente para instalação deverá possuir compatibilidade com os sistemas operacionais:

- macOS 12 (Monterey);
- macOS 11 (Big Sur);
- macOS 10.15 (Catalina);
- macOS 10.14 (Mojave);
- macOS 10.13 (High Sierra).

Suporte ao Apple Remote Desktop para instalação remota da solução;

Gerenciamento integrado à console de gerência central da solução;

Proteção em tempo real contra vírus, trojans, worms, cavalos-de-tróia, spyware, adwares e outros tipos de códigos maliciosos;

Permitir a verificação das ameaças da maneira manual e agendada;

Permitir a criação de listas de exclusões para pastas e arquivos que não serão verificados pelo antivírus;

Permitir ações de reparar arquivo ou colocar em quarentena em caso de infecções a arquivos;

Deve possuir mecanismo de proteção contra uso não autorizado no qual o agente deve ser protegido contra mudança do seu estado (não possibilitar que um administrador da estação de trabalho e notebook possa parar o serviço), bem como mecanismo para restaurar seu estado normal;

Deve possuir no mecanismo de autoproteção as seguintes proteções:

Proteção e verificação dos arquivos de assinatura;

Proteção dos processos do agente de segurança;

Proteção das chaves de registro do agente de segurança;

Proteção do diretório de instalação do agente de segurança.

Funcionalidade de HIPS – Host IPS e Host Firewall

Deve ser capaz de realizar a detecção/proteção contra exploração de vulnerabilidades nos seguintes sistemas operacionais:

- Windows 11 (x64);
- Windows 10 (x86/x64);
- Windows 8.1 (x86/x64).

Deve possuir módulo para proteção de vulnerabilidades com as funcionalidades de host IPS e host firewall;

As regras de vulnerabilidades deverão possuir a opção de desativar a regra de forma individual;

Todas as regras das funcionalidades de firewall e IPS de host devem permitir apenas detecção (log) ou prevenção (bloqueio);

Deve permitir ativar e desativar o produto sem a necessidade de remoção;

Deve permitir que o usuário altere as configurações de níveis de segurança e exceções;

Deverá possuir a possibilidade de configurar níveis diferentes de segurança podendo ser eles alto, médio e baixo;

O módulo de HIPS deverá possuir perfis pré-determinados baseados em performance e segurança;

O módulo de HIPS deverá possuir regras para proteger contra ameaças do tipo ransomware;

O módulo de HIPS deverá conter regras contra exploit, vulnerabilidades e genéricas protegendo contra ameaças conhecidas ou desconhecidas;

O módulo de HIPS deverá permitir que o administrador monitore apenas ou realize o bloqueio das tentativas de exploração de vulnerabilidades;

Deve suportar configuração de parâmetros de pacotes como quantidade máxima de conexões TCP e timeout para pacotes UDP;

Deve ter a capacidade de proteção contra exploração de vulnerabilidades do sistema operacional e de aplicações terceiras instaladas na estação de trabalho;

A lista de regras deve permitir que o administrador realize buscas e tenha rápida visibilidade do tipo da aplicação, em que modo a regra encontra-se (bloqueio ou monitoramento), CVE, CVSS score, quando aplicável.

Módulo para Controle de Aplicações

Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:

- Windows 8.1 (x86/x64);
- Windows 10 (x64);
- Windows 11 (x64).

As regras de controle de aplicação devem permitir as seguintes ações:

Permissão de execução;

Bloqueio de execução;

Bloqueio de novas instalações.

A regra de liberação para o controle de aplicação deverá permitir que o programa liberado efetue ou não a execução de outros processos;

As regras de controle de aplicação devem permitir o modo de apenas coleta de eventos (logs), sem a efetivação da ação da regra;

As regras de controle de aplicação devem permitir os seguintes métodos para identificação das aplicações:

- Assinatura SHA-1 e SHA-256 do executável;
- Atributos do certificado utilizado para assinatura digital do executável;
- Caminho lógico do executável;
- Base de assinaturas de certificados digitais válidos e seguros.

As regras de controle de aplicação devem possuir categorias pré-determinadas de aplicações;

As políticas de segurança devem permitir a utilização de múltiplas regras de controle de aplicações;

O módulo de controle de aplicativos deve possuir uma lista de aplicações mal-intencionadas para bloqueio e monitoramento tendo, pelo menos, as categorias de keyloggers, anonimizadores de proxy, P2P, crackers de senhas;

Deve permitir a busca por aplicações ou fabricante destas;

Deve possuir ferramenta para extrair o hash de um ou um grupo de executáveis, permitindo a importação destes hashes através de arquivo CSV.

Módulo de Detecção e Resposta

A solução deve ser compatível com os sistemas operacionais Windows, Linux e MacOS;

O fabricante deve implementar e organizar os ataques baseados no framework MITRE ATT&CK®, identificando técnicas e táticas dos ataques;

A solução deve possuir módulo de investigação e detecção integrados;

Deve fazer uso de inteligência artificial e inteligência de ameaças do fabricante da solução para analisar e correlacionar as atividades dos sensores do ambiente;

Possuir painéis que apresentem visualização executiva dos principais incidentes e atividades no ambiente com base nos usuários, aplicações acessadas e estações de trabalho;

Utilizar bases de inteligência de ameaças integrando relatórios de inteligência do fabricante e de terceiros para ajudar a identificar ameaças no ambiente;

Apresentar os alertas consolidados e correlacionados de ameaças para melhor investigação e resposta;

Fornecer a capacidade de realizar buscas avançadas para localizar dados ou objetos no ambiente para análise avançada de atividades ou detecções;

Capacidade de construir sequências de buscas poderosas para localizar os dados ou objetos em seu ambiente que você deseja examinar;

Deve prover diferentes métodos de pesquisa, filtros e uma linguagem de consulta do tipo Kibana para identificar, categorizar e recuperar os resultados da pesquisa;

Deve ser possível realizar buscas através de strings parciais, exatas, valores nulos, wildcards e caracteres especiais;

Permitir investigar os alertas gerados pelos modelos de detecção por meio de análise de impacto e análise de causa-raiz;

Deve consolidar e correlacionar diferentes modelos de ameaça relacionados a um único evento;

Deve permitir que as detecções sejam correlacionadas com módulos de servidores, rede e e-mail do próprio fabricante através de console dedicada, não sendo aceitas consoles de correlação de terceiros;

A console de correlação deve estar disponível na nuvem do próprio fabricante, o qual deve ser responsável pelas manutenções, atualizações e disponibilidade;

Deve possuir capacidade de encaminhar as atividades suspeitas identificadas nos servidores para a console de correlação centralizada;

O módulo de EDR deve atuar baseado em modelos de detecção de ataques avançados e furtivos;

Os logs de detecções devem estar disponíveis na console por, pelo menos, 30 dias;

A console de correlação centralizada deve possuir informações a respeito dos principais ataques que estão ocorrendo no mundo, quais plataformas e países são afetados, além de links para obter mais informações;

A console deve permitir Single Sign-On através de SAML ou padrão equivalente;

Deve exibir os eventos de forma a priorizar os alertas mais críticos para que o analista realize a investigação, como pontuações ou níveis de prioridade;

Deve ser possível criar usuários com permissões distintas, contendo no mínimo permissão total e permissão para realizar investigações;

Deve permitir habilitar ou desabilitar um determinado usuário sem excluí-lo da console;

Deve ser possível interagir com cada um dos objetos relacionados ao evento para análise avançada e resposta;

Deve destacar e organizar as atividades relacionadas a cada modelo de detecção por ordem cronológica, permitindo identificar a relação de cada atividade com os modelos de detecção;

Deve permitir o envio de notificações para os administradores através de e-mail, API e integrações com SIEMs;

Deve prover visualização em linha do tempo com informações dos eventos monitorados em cada estação de trabalho;

Deve permitir a visualização entre usuários, servidores, processos/comandos, arquivos e demais componentes correlacionados em determinado ataque;

Deverá informar com qual técnica e tática do MITRE ATT&CK framework o ataque está relacionado, além de possuir link direto para o site da organização;

A solução deve mostrar, pelo menos, o timestamp, objetos envolvidos (comandos, processos, usuários, servidores);

Ao clicar em quaisquer dos objetos, a solução deve permitir realizar buscas específicas pelo objeto ou ainda executar ações como executar investigações mais aprofundadas;

Deve informar qual o escopo de impacto ou dimensionar o impacto em servidores, estações de trabalho e usuários, indicando a quantidade de componentes afetados no ataque;

Deve permitir que o analista possa alterar o status dos incidentes de acordo com seu tratamento e indicar falsos positivos para a plataforma;

Deve permitir adicionar arquivos SHA-1, URLs, IPs ou domínios à lista de bloqueio dos sensores;

Deve permitir remover arquivos SHA-1, URLs, IPs ou domínios da lista de bloqueio dos sensores;

Deve permitir terminar processos ativos executados nas estações de trabalho e servidores;

Permitir coletar e fazer o download de um arquivo para investigação local detalhada;

Isolar a estação de trabalho desconectando-a da rede e permitindo se comunicar exclusivamente com a console de gerenciamento do fabricante;

Restaurar a conectividade da estação de trabalho com a rede;

Iniciar uma sessão de shell remoto na estação de trabalho selecionada para execução de comandos remotos para investigação;

Deve ser possível fazer o download do histórico da sessão após finalizar a sessão remota do shell na estação de trabalho para fins de auditoria.

SOLUÇÃO DE PROTEÇÃO DE SERVIDORES COM ABORDAGEM PROATIVA PARA RESPOSTA EFICAZ A INCIDENTES.

Características Gerais da Solução

A solução deverá ser compatível com pelo menos os seguintes sistemas operacionais:

- Windows Server 2000;
- Windows Server 2003 SP1 e 2003 R2 SP2;
- Windows Server 2008 e 2008 R2; Windows Server 2012 e 2012 R2;
- Windows Server 2016; Windows Server 2019; Windows Server 2022;
- Red Hat Enterprise 5, 6, 7 e 8;
- CentOS 5, 6, 7 e 8;
- AIX 6.1, 7.1 e 7.2;
- Oracle Linux 5, 6, 7 e 8;
- SUSE Linux Enterprise Server 10, 11, 12 e 15;
- Ubuntu 10, 12, 14, 16, 18 e 20;
- Debian 6, 7, 8, 9 e 10;
- Rocky Linux 8;
- Alma Linux 8;
- Cloud Linux 5, 6, 7 e 8;
- Solaris 10 1/13 Sparc;
- Solaris 10 1/13 (x86/x64);
- Solaris 11.2/11.3 Sparc;
- Solaris 11.2/11.3 (x86/x64);
- Solaris 11.4 (x86, x64 ou SPARC);
- Amazon Linux e Amazon Linux 2 (x64).

A solução deverá ser totalmente compatível e homologada com o ambiente Vmware;

A console de gerenciamento deverá ser em nuvem, permitindo o gerenciamento das políticas de segurança através da Internet;

A solução deverá ser gerenciada por console Web, compatível com pelo menos os browsers Internet Explorer, Google Chrome e Firefox; deve ainda suportar certificado digital para gerenciamento;

A solução deverá permitir a integração com pelo menos as seguintes plataformas de nuvem: Vmware vCloud, MS Azure e AWS;

Precisa ter a capacidade de controlar e gerenciar a segurança de múltiplas plataformas e sistemas operacionais, incluindo máquinas em nuvens externas, a partir de uma console única e centralizada do próprio fabricante;

A solução deverá permitir a entrega de agentes por pelo menos duas dentre as principais ferramentas de distribuição de software do mercado: Microsoft System Center Configuration Manager, Novel Zen Works e Puppet;

A console de administração deverá permitir o envio de notificações via SMTP;

Todos os eventos e ações realizadas na console de gerenciamento precisam ser gravados para fins de auditoria;

A solução deverá possuir a funcionalidade tags para identificar falsos positivos ou facilitar a visualização de determinados alertas;

A solução deverá permitir a criação de widgets para facilitar a administração e visualização dos eventos;

A solução deverá permitir que a distribuição de patterns e novos componentes possa ser efetuada por agentes de atualização espalhados pelo ambiente;

A solução precisa permitir a criação de relatórios, a criação e envio destes relatórios deverá ocorrer sob demanda, ou agendado com o envio automático do relatório via e-mail;

A solução deverá fornecer pelo menos dois tipos de relatórios nos seguintes formatos: PDF, CSV, XLS e RTF;

A solução precisa permitir que relatórios no formato PDF possam ser enviados com uma senha única para cada destinatário;

A solução deverá prover relatórios contendo no mínimo as seguintes informações: malware, regras de IPS aplicadas e Firewall;

Em caso de solução em nuvem, o ambiente do fabricante deverá fornecer alta disponibilidade; a solução de segurança deve ter a capacidade de identificar ataques entre contêineres;

Os usuários devem ter a capacidade de receber determinados papéis para administração como “acesso total” e “acesso parcial”, podendo ser customizado o que compõe o “acesso parcial”;

Quando configurado o acesso parcial, este deve permitir que um usuário tenha permissões de poder gerenciar a segurança de um único computador, podendo ainda definir em quais módulos de proteção será possível ou não editar ou criar novas políticas de segurança;

A comunicação entre a console de gerenciamento e os agentes deverá ser criptografada;

Cada agente deverá ter sua própria chave para criptografia, de modo que a comunicação criptografada seja feita de forma diferente para cada agente;

A console de gerenciamento deverá ter dashboards para facilidade de monitoração, as quais deverão ser customizadas pelo administrador em quantidade e período de monitoração;

Os agentes de atualização deverão buscar os updates das assinaturas e distribuí-las para os agentes; quando ocorrer a atualização, esta deverá ocorrer de modo absolutamente seguro utilizando-se SSL/TLS com o servidor de onde ela buscará as informações;

Os agentes para plataforma Microsoft deverão ser instalados por pacote MSI e posteriormente ativados pela console de gerenciamento de forma a proporcionar maior segurança ao ambiente, ou de forma automatizada através de script PowerShell;

Os agentes para plataforma Linux deverão ser instalados por pacote RPM ou DEB e posteriormente ativados pela console de gerenciamento de forma a proporcionar maior segurança ao ambiente, ou de forma automatizada através de bash script;

Em servidores Windows e Linux, a solução deverá permitir a atualização automática dos agentes após sua ativação;

Para servidores Linux, a solução deverá possibilitar a atualização automática da versão quando o agente reiniciar;

Para efeito de administração, a solução deverá avisar quando um agente se encontrar não conectado à sua console de gerenciamento;

Deve permitir a remoção automática de agentes inativos, definindo o período para, pelo menos: 1 semana, 1 mês e 12 meses;

A solução deve possuir a capacidade de criar políticas de forma global para todas as máquinas, por perfis e individualmente para cada host;

Cada perfil poderá ser atribuído para um host ou um conjunto de hosts;

A solução deverá vir com perfis pré-definidos e aptos a funcionarem de acordo com sua denominação; a solução deverá mostrar quais máquinas estão usando determinada política;

Os agentes deverão ser capazes de executar rastreamento nas máquinas onde estão instalados e, após isso, fornecer uma lista de todas as recomendações de segurança para os softwares que estejam instalados nas máquinas, bem como do sistema operacional;

Esses rastreamentos devem ocorrer de forma periódica a ser definida pelo administrador;

A solução deverá permitir a configuração de componentes de integração com o vCenter, a fim de permitir a sincronização das máquinas virtuais conectadas a ele;

Brechas de segurança descobertas deverão ser protegidas de forma automática e transparente, interrompendo somente o tráfego de rede malicioso;

O administrador do sistema de segurança deverá ter a possibilidade de não aplicar automaticamente a proteção para as vulnerabilidades escolhendo o perfil ou o host;

A solução deve possuir a capacidade de isolamento de placa de rede de forma que apenas uma fique funcionando de acordo com preferência do administrador;

A solução deverá ser capaz de aplicar políticas diferentes para placas de redes diferentes em um mesmo servidor;

A solução deverá ser capaz de executar bypass completo de rastreamento de tráfego de forma que os módulos não atuem em determinado tipo de conexão ou pacote;

A solução deverá ter a capacidade de se integrar com o Amazon SNS e os principais softwares de SIEMs contemplando, no mínimo: Splunk, IBM Qradar e HP ArcSight, de modo a permitir enviar os seus logs para essas soluções;

A solução deverá ter a possibilidade de enviar logs para SYSLOG servers;

Solução deverá permitir criar relatórios customizados de todas as suas funcionalidades;

Deve permitir enviar os relatórios para uma lista de contatos independente de login na console de administração;

As atualizações de assinaturas deverão ocorrer de forma agendada e automática, possibilitando ser até mesmo de hora em hora;

Após a atualização deve ser informado o que foi modificado ou adicionado;

Deve ser possível baixar as assinaturas na console de gerenciamento, mas não as distribuir aos clientes;

A console de gerenciamento deve apresentar a capacidade de gerar roll back de suas atualizações de regras;

A solução deverá ter capacidade de gerar pacote de autodiagnóstico de modo a coletar arquivos relevantes para envio ao suporte do produto;

Deverá ter a capacidade de colocar etiquetas para a ocorrência de determinados eventos de modo a facilitar o gerenciamento, relatórios e visualização;

No gerenciamento de licenças, deve ser informada quantidade contratada e quantidade em utilização de clientes;

Solução deverá ter mecanismo de procura em sua console de gerenciamento de modo que seja facilitada a busca de regras;

Deverá possuir a capacidade de classificar eventos para que facilite a identificação e a visualização de eventos críticos em servidores críticos;

Deverá possibilitar colocar etiquetas em eventos para que se possam visualizar apenas os eventos desejados;

O fabricante deverá participar do programa “Microsoft Application Protection Program” para obtenção de informações, de modo a permitir a criação de regras de proteção antes mesmo dos patches serem publicados pelo fabricante;

A console de gerenciamento deve se integrar com o Vmware vCloud, de modo a importar e sincronizar os objetos (hosts vmware e guests vm) para a console de gerenciamento da solução;

O fabricante da solução deverá manter programa de pesquisa em vulnerabilidades há, pelo menos, 5 anos;

A solução deve possuir API documentada para integração na esteira de automação;

A documentação da API deve conter exemplos prontos para implementação de determinadas funcionalidades, como cookbooks;

Precisa ter a capacidade de detectar e aplicar as regras necessárias dos módulos de IDS/IPS, Monitoramento de Integridade e Inspeção de Logs, para cada servidor, de forma automática e sem a intervenção do administrador;

A solução deve permitir desabilitar os módulos individualmente;

Precisa ter a capacidade de desabilitar as regras não mais necessárias dos módulos de IDS/IPS, Monitoramento de Integridade e Inspeção de Logs, para cada servidor, de forma automática e sem a intervenção do administrador.

Antimalware

A solução deve permitir a proteção contra códigos maliciosos através da instalação de agentes, permitindo rastrear ameaças em tempo real, varredura sob demanda e conforme agendamento, possibilitando

a tomada de ações distintas para cada tipo de ameaça;

A solução deve possibilitar a criação de listas de exclusão, para que o processo do antivírus não execute a varredura de determinados diretórios ou arquivos do SO;

A solução deve possuir listas de exclusão separadas por módulo da proteção antimalware, como exclusão das detecções por comportamento, exclusão por machine learning e exclusão por assinatura;

Em plataforma Windows, a solução deve permitir criar exclusões de escaneamento a partir do certificado digital das aplicações;

A solução deve possibilitar a verificação de ameaças dentro de arquivos compactados, efetuando a limpeza apenas de arquivos maliciosos em casos de detecção; a limpeza deve ocorrer sem a descompactação do arquivo;

Em servidores Windows, deve identificar e bloquear ameaças através de métodos de Machine Learning, quarentenando arquivos identificados;

A solução deverá possuir a funcionalidade de Monitoramento de Comportamento para detectar mudanças e atividades suspeitas não autorizadas;

A solução deverá oferecer escanear processos em memória em busca de malware;

O scan de arquivos comprimidos deverá ser de no mínimo 6 camadas de compressão;

O scan de arquivos comprimidos do tipo OLE deverá ser de no mínimo 20 camadas de compressão;

Para servidores Windows, a solução deverá permitir que o escaneamento agendado ocorra, ainda que o agente esteja offline na console de gerenciamento;

A solução deverá possuir ações pré-configuradas para cada tipo de ameaça detectada ou tomar uma ação baseada na configuração padrão da ferramenta;

Em servidores Windows, a solução deverá integrar-se com interface AMSI (Antimalware Scan Interface);

A solução deverá mostrar informação de data sobre o último scan agendado ou manual executado;

Possuir a capacidade de efetuar backup e restore de arquivos comprometidos por ransomware;

Deve possuir cache dos arquivos verificados de modo a evitar a redundância da varredura;

Deve possibilitar o controle do consumo de memória durante as varreduras, a fim de minimizar os impactos de desempenho no servidor;

A solução deve possuir opção para forçar a comunicação com o agente e coletar os respectivos logs;

Em servidores Windows, deve possuir capacidade de detectar ameaças por comportamento;

Deverá ter a possibilidade de escanear drivers de rede mapeados nos servidores.

Proteção Contra URLs Maliciosas

Deve permitir a proteção contra acesso a websites ou URLs consideradas maliciosas ou de baixa reputação;

A lista de URLs deve ser fornecida e atualizada automaticamente pelo fabricante, permitindo a consulta em uma base local ou na nuvem da reputação das URLs acessadas;

A solução deve permitir alterar o nível de sensibilidade para detecção de URLs maliciosas tendo, pelo menos, os níveis alto, médio e baixo;

Deve permitir a criação de listas de exclusão, permitindo que usuários acessem determinadas URLs especificadas pelo administrador do sistema;

Deve permitir configurar notificações personalizadas para detecções desse módulo, deixando a cargo do administrador exibir ou não tais notificações;

Deverá ter capacidade de identificar acessos a URLs maliciosas além das portas padrão 80 e 443;

A solução deve permitir que o administrador reclassifique uma URL através do site do fabricante para evitar falsos positivos;

A proteção deve possibilitar proteção através da instalação de agente de segurança do fabricante da solução de segurança.

Firewall

Operar como firewall de host, através da instalação de agente nos servidores protegidos;

Precisa ter a capacidade de controlar o tráfego baseado no endereço MAC, frame types, tipos de protocolos, endereços IP e intervalo de portas;

Precisa ter a capacidade de controlar conexões TCP baseado nas flags TCP;

Precisa ter a capacidade de definir regras distintas para interfaces de rede distintas;

A solução deverá ser capaz de reconhecer e possibilitar o bloqueio de endereços IP que estejam realizando Network Scan, Port Scan, TCP Null Scan, TCP FYNSYN Scan, TCP Xmas Scan e Computer OS Fingerprint por até 30 minutos;

Precisa ter a capacidade de implementação de regras em determinados horários que podem ser customizados pelo administrador;

Precisa ter a capacidade de definição de regras para contextos específicos;

Para facilitar a criação e administração de regras de firewall, as mesmas poderão se apoiar em objetos que podem ser lista de IPs, lista de MACs, lista de portas;

Regras de firewall poderão ou não ser válidas de acordo com o contexto em que a máquina se encontra (por exemplo, se está no domínio ou não);

Regras de firewall poderão ou não ser válidas de acordo com agendamento por horário ou dia da semana;

O firewall deverá ser stateful bidirecional;

O firewall deverá permitir liberar ou apenas logar eventos;

O firewall deverá ser passível de criação de regras através do protocolo, origem do tráfego, frame type, TCP header flags, destino e direção;

As regras de firewall deverão ter as seguintes ações, ou equivalentes: Allow, log only, bypass, force allow, deny;

A solução, para facilidade de administração, deverá utilizar o conceito de regras implícitas para a regra ALLOW, negando o tráfego para todo o restante que não estiver liberado;

As ações também deverão ser possíveis de terem prioridades diferentes, sendo que a prioridade maior prevalece sobre a prioridade menor;

Deverá realizar pseudo stateful em tráfego UDP; deverá logar a atividade stateful;

Deverá permitir limitar o número de conexões entrantes e o número de conexões de saída de um determinado computador;

Deverá permitir limitar o número de meias conexões vindas de um computador; deverá prevenir ack storm;

Deverão existir regras default que possam ser utilizadas como modelo para a criação e adição de novas regras;

Deverá identificar escaneamentos ativos de porta ou da rede, bloqueando o IP ofensor por um período de tempo configurado pelo administrador;

Deverá permitir criar lista de exceções para identificar os IPs autorizados a realizar varreduras de portas ou da rede;

Poderá atuar no modo em linha para proteção contra-ataques ou modo escuta para monitoração e alertas.

Proteção de Vulnerabilidades de SO e Aplicações

Precisa ter a capacidade de detectar e bloquear qualquer conexão indesejada que tente explorar vulnerabilidades do SO e demais aplicações;

Precisa ter a capacidade de varrer o servidor protegido detectando o tipo e versão do SO, detectando também as demais aplicações, recomendando e aplicando automaticamente regras IDS/IPS que blindem vulnerabilidades existentes no SO e aplicações; esta varredura deverá poder ser executada sob demanda ou agendada;

A solução deverá conter regras pré-definidas para detecções de ransomware para as principais famílias deste tipo de malware;

Precisa ter a capacidade de detectar uma conexão maliciosa, com a possibilidade de bloquear esta conexão;

Precisa conter regras de defesa para blindagem de vulnerabilidades e ataques que explorem os seguintes sistemas operacionais: Windows 2003, 2008, 2012, 2016, 2019, Linux Red Hat, Suse, CentOS, Ubuntu, Debian, Solaris, AIX, além de regras para aplicações padrão de mercado, incluindo Microsoft IIS, SQL Server, Microsoft Exchange, Oracle Database, Adobe Acrobat, Mozilla Firefox, Microsoft Internet Explorer, Google Chrome e Web Server Apache;

Precisa ter a capacidade de armazenamento do pacote capturado quando detectado um ataque;

Deverá possibilitar a criação de regras de IPS customizadas, para proteger aplicações desenvolvidas pelo cliente;

Precisa possuir a capacidade de detectar e controlar conexões de aplicações específicas incluindo Team Viewer, programas P2P e instant messaging;

Precisa ter a capacidade de detectar e bloquear ataques em aplicações web tais como SQL Injection e Cross Site Scripting; deverá ainda existir a possibilidade de captura do pacote relacionado ao ataque para fins de investigação do incidente;

Deverá permitir customização avançada e criação de novas regras de proteção de aplicações web, protegendo contra vulnerabilidades específicas de sistemas web legados e/ou proprietários;

Ser capaz de permitir ou negar métodos utilizados por webservers por regras de IPS;

Regras de IDS/IPS poderão ou não ser válidas de acordo com o contexto em que a máquina se encontra (por exemplo, se está no domínio ou não)

Regras de IDS/IPS poderão ou não ser válidas de acordo com agendamento por horário ou dia da semana;

Deverá ser capaz de inspecionar tráfego criptografado de entrada;

Deverá inspecionar tráfego de aplicações web em servidores buscando identificar: SQL injection, cross-site script, tamanho de URI fora de padrão, caracteres fora de padrão para requisição de URI, double decoding exploit;

As regras de blindagem contra vulnerabilidades deverão conter links com referências externas, isto quando aplicável, explicando a vulnerabilidade do fabricante ou CVE relacionado;

Deverá possibilitar a criação de regras manuais para o bloqueio de tráfego customizado, como por exemplo: bloquear acesso a um determinado website ou bloquear acesso de uma aplicação X;

Deverá possibilitar a criação de regras manuais baseadas em padrão XML, forma de assinatura ou padrões que possuam começo e fim coincidentes;

Deverá bloquear tráfego por aplicação independente da porta que a aplicação utilize, de modo que a aplicação não consiga comunicar na rede, como por exemplo, bloqueio de tráfego de um determinado web browser ou aplicação de backup;

Solução deve ser capaz de habilitar modo debug na coleta dos pacotes, de forma a capturar o tráfego anterior e posterior ao que foi bloqueado para facilidade de análise;

As regras de IPS deverão obrigatoriamente ter descrições de seu propósito;

As regras de IPS poderão atuar detectando ou bloqueando os eventos que as violem, de modo que o administrador possa optar por qual ação tomar;

As regras de IPS de vulnerabilidade deverão apresentar severidade baseada em CVEs; as regras de IPS poderão ter sua capacidade de log desabilitado;

As regras de IPS quando disparadas poderão ter a possibilidade de emitir um alerta;

As regras devem ser atualizadas automaticamente pelo fabricante;

Poderá atuar no modo em linha para proteção contra-ataques ou modo escuta para monitoração e alertas.

Monitoramento de Integridade

A solução deverá permitir a implantação nas plataformas Linux, Microsoft, Solaris, HP-UX, AIX, através da instalação de agentes;

Precisa ter a capacidade de detectar mudanças de integridade em arquivos e diretórios do SO e aplicações terceiras;

Precisa ser capaz de detectar mudanças no estado de portas em sistemas operacionais Linux;

Precisa ter a capacidade de monitorar o status de serviços e processos do sistema operacional;

Precisa ter a capacidade de monitorar mudanças efetuadas no registro do Windows;

Precisa ter a capacidade de criação de regras de monitoramento em chaves de registro, diretórios e subdiretórios e customização de XML para criação de regras avançadas;

Precisa ter a capacidade de varrer o sistema operacional e aplicações, recomendando e aplicando automaticamente regras de monitoramento de acordo com o resultado desta varredura; esta varredura deverá poder ser executada sob demanda ou agendada;

O monitoramento poderá ser realizado em tempo real ou utilizando scans periódicos para detectar mudanças de integridade;

Deverá alertar toda vez que uma modificação ocorrer em tempo real para ambiente Windows e pseudo real-time para ambiente Linux;

Deverá logar e colocar em relatório todas as modificações que ocorram;

As regras de monitoramento de integridade deverão ser atualizadas pelo fabricante ou melhoradas de forma automática;

Deverá poder classificar as regras de acordo com severidade para melhor verificação nos logs e recebimento de alertas;

Deverá possibilitar escolher o diretório onde o arquivo será monitorado e incluir ou não incluir determinados tipos de arquivos dentro desse mesmo diretório;

Algumas regras podem ser modificadas pelo administrador para adequação ao seu ambiente.

Inspeção de Logs

A solução deverá permitir sua implantação nas plataformas Linux, Microsoft, Solaris, HP-UX, AIX;

Precisa ter a capacidade de monitorar e inspecionar arquivos de log do sistema operacional e demais aplicações, gravando uma cópia deste log em um banco de dados externo e notificando o administrador sobre eventos suspeitos;

Precisa ter a capacidade de varrer o sistema operacional e aplicações, recomendando e aplicando automaticamente regras de inspeção de logs de acordo com o resultado desta varredura; esta varredura deverá poder ser executada sob demanda ou agendada;

Precisa permitir a criação de regras de inspeção de logs adicionais para auditoria de logs de aplicações terceiras;

Precisa permitir a customização de regras existentes, adicionando, removendo ou modificando regras de inspeção de logs;

Deverá rastrear e indicar/sugerir ao administrador do sistema quais softwares estão instalados e que possuem logs passíveis de inspeção;

Deverá possibilitar a criação de regras de inspeção de logs para aplicações customizadas;

Deverá ter inteligência para que a cada violação relevante no log inspecionado que possa comprometer a segurança do ambiente ou do servidor seja alertada;

Deverá ter inteligência para que a cada violação relevante no log inspecionado que seja suspeita no servidor seja alertada;

Deverá logar cada violação e colocar em relatório todas as violações relevantes que ocorram;

As regras poderão ser modificadas por severidade de ocorrência de eventos;

As regras devem se atualizar automaticamente pelo fabricante;

Permitir modificação pelo administrador em regras para adequação ao ambiente.

Controle de Aplicações

A solução deverá permitir sua implantação nas plataformas Linux e Microsoft Windows;

O controle de aplicações deverá ser realizado através de hash, suportando no mínimo MD5, SHA1 e SHA256;

O agrupamento dos eventos deverá ser realizado pelo menos por hash ou por máquina;

A console deverá exibir eventos de no mínimo 30 dias;

A solução deverá possuir um mecanismo ao qual permita a execução de aplicações e scripts automaticamente, sem intervenção manual, por um determinado período que deve ser no máximo 10 horas;

A solução deverá possuir no mínimo as funcionalidades de bloquear o que não for permitido explicitamente e permitir o que não for bloqueado explicitamente.

Detecção e Resposta

A solução deve ser compatível com Linux e Windows Server 2008 R2 e superiores;

A solução deve possuir módulo de investigação e detecção integrados;

Deve permitir que as detecções sejam correlacionadas com módulos de endpoint, rede e e-mail do próprio fabricante através de console dedicada; não serão aceitas consoles de correlação de terceiros;

A console de correlação deve estar disponível na nuvem do próprio fabricante, o qual deve ser responsável pelas manutenções, atualizações e disponibilidade;

Deve possuir capacidade de encaminhar as atividades suspeitas identificadas nos servidores para a console de correlação centralizada;

O módulo de EDR deve atuar baseado em modelos de detecção de ataques avançados e furtivos;

Os logs de detecções devem estar disponíveis na console por, pelo menos, 30 dias;

A console de correlação centralizada deve possuir informações a respeito dos principais ataques que estão ocorrendo no mundo, quais plataformas e países são afetados, além de links para obter mais informações;

A solução deve permitir realizar buscas em todos os dados de atividades enviadas pelos servidores e demais sensores que estejam conectados na console, ainda que estas não sejam detectadas como maliciosas;

A console deve permitir o Single Sign-On através de SAML ou padrão equivalente;

Deve ser possível criar usuários com permissões distintas, contendo no mínimo permissão total e permissão para realizar investigações;

Deve permitir habilitar ou desabilitar um determinado usuário sem excluí-lo da console;

Deve permitir o envio de notificações para os administradores através de e-mail, API e integrações com SIEMs;

Deve prover visualização em linha do tempo com informações dos eventos monitorados em cada servidor;

Deve permitir a visualização entre usuários, servidores, processos/comandos, arquivos e demais componentes correlacionados em determinado ataque;

Deverá informar com qual técnica e tática do MITRE ATT&CK framework o ataque está relacionado, além de possuir link direto para o site da organização;

A solução deve mostrar, pelo menos, o timestamp, objetos envolvidos (comandos, processos, usuários, servidores);

Ao clicar em quaisquer dos objetos, a solução deve permitir realizar buscas específicas pelo objeto ou ainda executar ações como executar investigações mais aprofundadas.

SERVIÇO DE SUPORTE PROATIVO, CORRETIVO E PARA RESPOSTA A INCIDENTES

Deverá ser oferecido suporte técnico da Contratada, com a possibilidade de abertura de chamados, das 7h00 às 20h00, em dias úteis, para a resolução de problemas. É importante destacar que os serviços de suporte técnico devem contemplar as manutenções corretivas e evolutivas para a solução contratada e não podem acarretar custos adicionais ao CONTRATANTE, além do que foi previamente acordado.

A empresa contratada deve encaminhar o chamado para o suporte do fabricante sempre que necessário, seja devido à criticidade, impacto ou urgência do problema, ou caso seja necessário o envolvimento direto do fabricante no processo de correção. É imprescindível que seja fornecido acesso ao site do fabricante para acompanhamento dos chamados, acesso à base de conhecimento e aos fóruns relacionados à solução.

Os serviços de suporte técnico abrangem:

Manutenção preventiva, manutenção corretiva, esclarecimento de dúvidas e reparação de problemas na solução.

Elaboração de relatórios, estudos e diagnósticos sobre o ambiente.

Transferência de conhecimento aos técnicos da Contratante referente aos problemas vivenciados e às soluções aplicadas, na forma a ser determinada pelas partes.

Realização de instalação, atualização e configuração de novas versões dos produtos após a disponibilização das atualizações tecnológicas pelo fabricante.

O suporte técnico deve contemplar o atendimento para sanar dúvidas relacionadas com instalação, configuração e uso do software ou para correção de problemas, em especial na configuração de parâmetros, falhas, erros, defeitos ou vícios identificados no funcionamento da solução.

O suporte técnico deve contemplar, quando for o caso, atendimento a eventual problema de instalação ou configuração de softwares básicos e de infraestrutura de TIC (sistemas operacionais, servidores de banco de dados, servidores de aplicação, etc.) necessários ao funcionamento da solução.

Deve contemplar também a atualização de versões do software aplicativo, as quais incorporam correções de erros ou problemas registrados e melhorias implementadas pela fabricante, num empacotamento estável do sistema. O serviço de atualização de versão tem por finalidade assegurar a devida atualização da solução durante o período de vigência da garantia. Refere-se ao fornecimento de novas versões e releases da solução lançados no período. A cada nova liberação de versão e release, serão disponibilizados em formato digital manuais e demais documentos técnicos, bem como nota informativa das funcionalidades implementadas. Em caso de lançamento de patch de correção, a CONTRATADA deverá comunicar o fato ao CONTRATANTE e indicar a forma de obtenção e os defeitos que serão corrigidos pelo patch. Em ambos os casos, a comunicação deve ser feita no prazo de até 30 dias, a contar do lançamento de nova versão ou solução de correção.

Deverá ser prestado suporte técnico remoto com atendimento mediante registro de chamados em página de website, em sistema fornecido pela CONTRATADA e/ou pelo fabricante; e também através de contato telefônico. Esse serviço destina-se a esclarecimento de dúvidas e resolução de problemas relacionados à configuração e uso dos componentes da solução CONTRATADA.

A CONTRATADA auxiliará o CONTRATANTE na reinstalação das ferramentas, caso seja necessário, ao longo do tempo de garantia da ferramenta.

A CONTRATADA deverá disponibilizar os seguintes canais de acesso ao suporte técnico: Portal Web; E-mail; Central 0800; e/ou Telefone fixo.

O atendimento deve ser contínuo, 24 horas por dia, 7 dias por semana, durante todo o ano, incluindo feriados, em língua portuguesa. O início do atendimento e o prazo de solução devem ser determinados de acordo com o nível de severidade exigido para o caso, conforme os índices de criticidade abaixo:

Criticidade	Descrição	Prazo Máximo de Atendimento	Prazo Máximo de Restauração de Serviço	Glosa (por evento) para eventual descumprimento

Severidade 1 (Alta)	Sistema parado ou produto inoperante com impacto nas operações críticas de negócio. Exemplos: Servidor de produção ou outro sistema inicial está inativo. Parte substancial dos dados essenciais corre risco de perda ou corrupção. As operações relacionadas ao negócio foram afetadas, falha que compromete a integridade geral do sistema ou dos dados.	Em até 2 horas deve ter um técnico do fornecedor on-site.	Em até 8 horas	10%
		Em até 4 horas deve ter um técnico do fornecedor on-site.	Entrega da Solução pelo fabricante em até 6 dias.	
Severidade 2 (Média/Alta)	Alto impacto no ambiente de produção ou grande restrição de funcionalidade. Exemplo: Ocorreu um problema no qual um recurso importante foi gravemente danificado. As operações podem continuar de forma limitada, embora a produtividade a longo prazo possa ser afetada negativamente.	Em até 4 horas deve ter um técnico do fornecedor on-site.	Em até 4 horas deve ter um técnico do fornecedor on-site.	7,50%
		Em até 2 horas um Engenheiro de Suporte do fabricante deve iniciar o atendimento através de transferência ao telefone ou retorno de chamada. Gerente técnico do fabricante deve estar disponível 24x7 e ser automaticamente notificado na abertura do caso.	Em até 16 horas	
			Entrega da Solução pelo fabricante em até 10 dias.	
Severidade 3	O defeito que não gera impacto ao negócio. Exemplo: Ocorreu um erro que causou impacto negativo limitado nas operações.	Um técnico do fornecedor on-site ou atendimento remoto.	Em até 24 horas.	5%
		Em até 6 horas um Engenheiro de Suporte do fabricante entra em contato.	Entrega da Solução pelo fabricante em até 15 dias ou na próxima atualização do Software.	
Severidade 4 (Baixa)	O problema é pequeno, ou de documentação. Exemplos: O problema não afetou as operações da contratante negativamente; Encaminhamento de solicitações e ou sugestões para novos recursos ou aprimoramento do software licenciado.	Em até 12 horas um técnico do fornecedor entra em contato.	Em até 12 horas um técnico do fornecedor entra em contato.	2%
		No mesmo dia ou no próximo dia útil comercial.	No mesmo dia ou no próximo dia útil comercial.	

Para cada chamado de suporte categorizado como grau de severidade 1, o recurso previsto na tabela acima deverá ser notificado e iniciará o auxílio na condução do processo internamente junto ao fabricante. É importante destacar que todos os prazos para atendimento da garantia começarão a ser contados a partir da abertura do chamado, independentemente de ter sido feito via telefone, e-mail, site da contratada ou do

fabricante. Além disso, o período de suporte deve estar diretamente atrelado ao período de garantia da solução.

Dentro do prazo máximo de atendimento, cabe ao fornecedor dar início, junto ao contratante, às providências que serão adotadas para a solução do chamado. Considera-se plenamente solucionado o problema quando os sistemas/serviços forem restabelecidos sem restrições, ou seja, quando não se tratar de uma solução paliativa.

Para os chamados de severidades 1 e 2, os serviços de atendimento de garantia não podem ser interrompidos até o completo restabelecimento de todas as funções do sistema paralisado, mesmo que isso exija períodos noturnos e dias não úteis (sábados, domingos e feriados). Além disso, os chamados de garantia de severidades 1 e 2 devem contar com suporte in loco da contratada para agilizar o restabelecimento do serviço.

O fornecedor emitirá um relatório, sempre que solicitado pelo contratante, em formato eletrônico, preferencialmente em arquivo texto, contendo informações analíticas e sintéticas dos chamados da garantia abertos e fechados no período. Esse relatório deve incluir:

- Quantidade de ocorrências (chamados) registradas no período.
- Número do chamado registrado e nível de severidade, incluindo reaberturas.
- Data e hora de abertura.
- Data e hora de início e conclusão do atendimento.
- Identificação do técnico do contratante que registrou o chamado.
- Identificação do técnico do contratante que atendeu o chamado da garantia.
- Descrição do problema.
- Descrição da solução.
- Informações sobre eventuais escalonamentos.
- Resumo da lista de chamados concluídos fora do prazo de solução estabelecido.
- Total de chamados no mês e o total acumulado até a apresentação do relatório.

Deverá ser emitido um relatório de histórico e revisão de casos, fornecido pelo gerente técnico do fabricante, sob os chamados abertos ou de responsabilidade do fabricante.

Deverá ser emitido um relatório de histórico e revisão de casos, fornecido pelo gerente técnico do fabricante, sob os chamados abertos ou de responsabilidade do fabricante. 5.4.18. Não se encaixam nos prazos descritos nos itens referentes aos níveis de criticidade, problemas cuja solução dependa de correção de falhas (bugs) ou da liberação de novas versões e patches de correção, desde que comprovados pelo fabricante da solução.

Para esses problemas, o fornecedor deverá, nos prazos estabelecidos nos níveis de criticidade, restabelecer o ambiente, através de uma solução de contorno e informar ao contratante, em um prazo máximo de 24 (vinte e quatro) horas, quando a solução definitiva será disponibilizada para o contratante.

O serviço de suporte proativo, corretivo para incidentes compreende um conjunto abrangente de atividades destinadas a assegurar o pleno funcionamento e a continuidade operacional de sistemas, soluções ou serviços. Este serviço é estrategicamente desenhado para atender às demandas

TRIBUNAL DE JUSTIÇA DO ESTADO DO ACRE
Rua Tribunal de Justiça, s/n, Via Verde
69.919-631 - Rio Branco-AC - (68) 3212-8277

dinâmicas do ambiente tecnológico, oferecendo suporte preventivo, corretivo e uma resposta ágil a incidentes de segurança.

Todo o Serviço de Suporte deverá ser prestado por profissional certificado pelo Fabricante da Solução, em nível compatível com a prestação do serviço. Deverá ser apresentada comprovação da certificação dos profissionais responsáveis no ato da assinatura do contrato.

Deverá disponibilizar um serviço preventivo de verificação e atualização de versões ou correções (patches) que se fizerem necessários, específicos para a solução ofertada;

Deverá prestar suporte a todos os componentes de software fornecidos que forem necessários para a implementação e utilização da solução.

Suporte Proativo:

O suporte proativo deverá antecipar potenciais problemas, identificando e resolvendo questões antes mesmo que impactem o desempenho e a segurança do ambiente;

A contratada deverá notificar a contratante sobre atualizações de segurança, patches e correções assim que estiverem disponíveis, caso autorizado aplicar as atualizações de segurança e evolutiva dos produtos;

Deverá realizar análises preditivas, buscando otimizar a performance e prevenir falhas nos produtos, além de detectar padrões que possam indicar uma possível violação de segurança, proporcionando um ambiente mais estável e seguro;

Deverá realizar avaliações regulares de riscos para identificar possíveis vulnerabilidades e pontos fracos nos sistemas e, implementar medidas corretivas com base nos resultados das avaliações de riscos;

Realizar auditorias regulares para garantir que as melhores práticas e os controles de segurança estejam operacionais e, utilizar resultados de auditorias para implementar melhorias contínuas;

A CONTRATADA deverá apresentar relatório contendo as ações adotadas para a solução do problema.

Suporte Corretivo:

Este componente concentra-se na solução de problemas ou incidentes. O suporte corretivo atua de forma ágil para restabelecer a funcionalidade normal do sistema, minimizando impactos negativos e mantendo a continuidade operacional;

Serviço Especializado de Suportes Corretivo para 24 meses. Serviço de Suporte especializado para ajustes, correções e configurações da solução a ser fornecida. Neste serviço deverá estar incluso todo tipo de suporte para funcionamento da solução;

A contratada deverá:

Implementar um sistema de abertura de chamados, para registrar, rastrear e priorizar incidentes e requisições de suporte;

Atribuir números de caso exclusivos para facilitar a comunicação e o acompanhamento;

Garantir disponibilidade 24/7 para responder a incidentes críticos.

Deverá apresentar relatório contendo as ações adotadas para a solução do problema.

Resposta a Incidentes:

O serviço de resposta a incidentes deverá lidar com eventos imprevistos, como violações de segurança, falhas críticas ou interrupções inesperadas. deverá ser realizada por profissionais especializados e certificados pelo fabricante;

Deverá realizar investigações para determinar a natureza, origem e impacto de incidentes de segurança;

Desenvolver planos de mitigação e estratégia de recuperação para minimizar o impacto de incidentes;

Elaborar relatórios detalhados sobre os incidentes, incluindo ações tomadas e recomendações de melhorias.

SERVIÇO DE IMPLANTAÇÃO

Nesta etapa, compreende-se a instalação e configuração da solução contratada, contados a partir da emissão da Ordem de Serviço (OS);

O serviço de implantação abrange integralmente as fases essenciais para a integração, instalação e configuração da solução contratada, alinhando-se precisamente com as especificações técnicas e requisitos predefinidos. Esta abordagem abarca desde o planejamento inicial até a conclusão efetiva, assegurando uma transição suave dos processos existentes para a nova solução;

O Plano de Implantação assume a forma de um documento fundamental que consolida a estratégia para instalação, configuração e entrega da solução contratada. Sua importância reside em orientar e alinhar as atividades, garantindo eficiência e uma implementação adequada da solução conforme os requisitos estabelecidos;

O documento deverá conter no mínimo os requisitos de ambiente tecnológicos necessários para a instalação das licenças, cronograma e detalhamento das atividades a serem realizadas, topologia do ambiente pós instalação da solução, matriz de responsabilidade, plano de comunicação;

Durante esta etapa, a equipe da Contratada deverá estar presente nos horários de instalação definidos pelo Contratante. As atividades de instalação e configuração poderão ser realizadas, conforme necessário, em horário comercial, período noturno ou final de semana;

O Contratante disponibilizará a infraestrutura de hardware e software necessária e já existente em seu ambiente, incluindo o ambiente virtualizado, sistema operacional, banco de dados, e outros, para a instalação e configuração da solução durante esta etapa.

SERVIÇO DE CAPACITAÇÃO E REPASSE DE CONHECIMENTO

A CONTRATADA deverá realizar serviço de capacitação técnica e repasse de conhecimento aos servidores da CONTRATANTE que atuarão diretamente na operação, administração, monitoramento e acompanhamento da solução de segurança de endpoints com abordagem de detecção e resposta a incidentes.

A capacitação deverá abranger todos os softwares e módulos integrantes da solução contratada, contemplando, no mínimo, os seguintes conteúdos:

- Instalação do módulo de gerenciamento central;
- Instalação e ativação dos agentes de proteção em estações de trabalho e servidores;
- Descrição, parametrização e configuração de todas as funcionalidades contratadas;
- Administração da console de gerenciamento;
- Criação e gestão de políticas de segurança;
- Monitoramento de eventos e análise de alertas;
- Investigação de incidentes e análise de causa-raiz;
- Procedimentos de contenção e resposta a ameaças;
- Geração e interpretação de relatórios;
- Integração com outros mecanismos de segurança, quando aplicável;
- Melhores práticas de mercado para otimização da solução e redução de riscos operacionais;
- Resolução de problemas (troubleshooting) e procedimentos de suporte.

O treinamento deverá possuir carga-horária mínima de 40 (quarenta) horas, podendo ser estruturado em expedientes de até 4 (quatro) horas diárias, em horário comercial, conforme conveniência da contratante.

A capacitação poderá ser realizada na modalidade presencial, nas dependências da CONTRATANTE, ou virtual (remota síncrona), para 1 (uma) turma, conforme definido pela Administração no momento da execução contratual, devendo ser ministrada por profissional devidamente certificado pelo fabricante da solução e comprovadamente habilitado para condução de treinamento técnico oficial.

O treinamento deverá conter parte teórica e prática, incluindo simulações de cenários reais de incidentes de segurança, de modo a proporcionar domínio operacional completo da ferramenta.

O treinamento será demandado pela CONTRATANTE após a efetiva implementação, configuração e estabilização da solução no ambiente do Poder Judiciário do Estado do Acre, ocasião em que as partes acordarão formalmente o cronograma de execução.

Deverá ser fornecido material didático completo, preferencialmente com conteúdo oficial do fabricante, em formato digital. O material deverá contemplar o conteúdo programático ministrado, servindo como apoio ao aprendizado teórico e prático. Caso o fabricante não disponibilize material oficial em língua portuguesa, será admitido material em língua inglesa, mediante justificativa formal.

As datas e horários de realização do treinamento deverão ser previamente acordados com a CONTRATANTE, respeitando o planejamento institucional.

Todos os custos relacionados à realização da capacitação, incluindo instrutor, material didático, infraestrutura tecnológica para modalidade remota (quando aplicável), deslocamento, hospedagem, alimentação e quaisquer outras despesas necessárias à execução do serviço, serão de exclusiva responsabilidade da CONTRATADA.

A capacitação tem por objetivo assegurar a autonomia técnica da equipe do PJAC, elevar o nível de maturidade em segurança cibernética institucional e garantir a adequada utilização, administração e sustentação da solução ao longo de todo o seu ciclo de vida contratual.

A solução de segurança a ser adotada deverá possuir arquitetura tecnológica capaz de assegurar níveis adequados de disponibilidade, autenticidade, integridade e confiabilidade das informações produzidas, processadas e armazenadas nos meios tecnológicos do Poder Judiciário do Estado do Acre (PJAC), com foco na proteção de endpoints (estações de trabalho e servidores).

A solução deverá dispor de arquitetura centralizada de gerenciamento, permitindo administração unificada, simplificada e integrada de todos os endpoints protegidos, por meio de console único, com visibilidade ampla da postura de segurança do ambiente institucional.

Deverá suportar mecanismos de avaliação de reputação de arquivos, tanto para arquivos locais quanto para conteúdos acessados via web, possibilitando a identificação preventiva de arquivos maliciosos e impedindo sua execução ou abertura nos endpoints.

A solução deverá empregar técnicas de aprendizado de máquina (Machine Learning) e análise comportamental (Behavioral Analysis), de forma a identificar padrões anômalos e comportamentos suspeitos, permitindo a detecção de ameaças conhecidas e desconhecidas, inclusive aquelas que não dependem de assinaturas tradicionais.

Deverá contemplar mecanismos de mitigação de exploração de memória, protegendo os endpoints contra ataques que explorem vulnerabilidades de memória, tais como injeção de código malicioso, estouro de buffer e técnicas similares, frequentemente utilizadas em ataques avançados.

A arquitetura deverá permitir a redução da complexidade operacional, oferecendo estrutura integrada de segurança, com políticas centralizadas, visibilidade consolidada dos dispositivos monitorados e simplificação das atividades de administração, operação e resposta a incidentes.

A solução deverá possibilitar gerenciamento centralizado de vulnerabilidades e patches de segurança, permitindo identificar exposições conhecidas nos endpoints e apoiar a aplicação de correções de forma organizada, eficiente e alinhada às políticas institucionais.

Deverá dispor de mecanismos de resposta automática ou orquestrada a incidentes, possibilitando ações como isolamento de dispositivos, bloqueio de processos maliciosos e contenção de ameaças, com o objetivo de minimizar o tempo de exposição e reduzir o impacto de incidentes de segurança.

A arquitetura tecnológica deverá ser escalável e flexível, permitindo a ampliação do número de endpoints protegidos e a evolução funcional da solução sem necessidade de reestruturação significativa,

acompanhando o crescimento do parque computacional do PJAC.

Por fim, a solução deverá ser compatível com integrações com outras camadas de segurança existentes ou futuras, viabilizando uma arquitetura de defesa em profundidade e fornecendo subsídios técnicos para análises contínuas de risco e fortalecimento da postura de segurança institucional.

1.3.3.2. Requisitos de Capacitação:

A contratada deverá realizar repasse de conhecimento à equipe técnica da contratante, com carga horária mínima de 40 (quarenta) horas, abrangendo instalação, configuração, administração, monitoramento, investigação e resposta a incidentes da solução de segurança de endpoints.

O treinamento deverá contemplar conteúdos teóricos e práticos, ser ministrado por profissional certificado pelo fabricante e ocorrer após a implantação da solução, em cronograma previamente acordado entre as partes.

Deverá ser fornecido material didático oficial do fabricante, preferencialmente em língua portuguesa, sendo todos os custos relacionados à capacitação de responsabilidade exclusiva da contratada.

1.3.3.3. Requisitos de Manutenção:

A CONTRATADA será responsável por fornecer suporte técnico especializado e garantia de atualização da solução pelo período mínimo de 24 (vinte e quatro) meses, contados a partir da emissão do Termo de Recebimento Definitivo.

A garantia deverá abranger integralmente o licenciamento da solução, seus módulos, componentes, agentes instalados nos endpoints e demais funcionalidades contratadas, não se limitando ao término da vigência contratual, quando houver aditivos relacionados à renovação ou ampliação das licenças.

A garantia deverá incluir, obrigatoriamente:

- Atualização de versões dos softwares fornecidos, sempre que disponibilizadas novas versões pelo fabricante;
- Atualização da solução nos casos de substituição tecnológica ou descontinuidade do produto originalmente fornecido, ainda que não se trate de substituição direta, assegurando a continuidade da proteção contratada;
- Correções de falhas (bugs), vulnerabilidades ou defeitos identificados na solução, incluindo aplicação de patches de segurança e demais atualizações necessárias à preservação da integridade e segurança do ambiente.

O suporte técnico deverá contemplar atendimento remoto para diagnóstico, orientação e resolução de incidentes relacionados ao funcionamento da solução, bem como apoio na análise de eventos de segurança quando houver falhas atribuíveis ao produto.

A garantia deverá ser prestada durante todo o período contratual e eventuais aditivos relacionados à atualização das licenças e proteção, assegurando a continuidade da cobertura de segurança para os endpoints protegidos.

Caso a solução envolva fornecimento de equipamentos físicos (appliances ou componentes dedicados), a CONTRATADA deverá substituir, no prazo máximo de 15 (quinze) dias úteis, os equipamentos que apresentarem, no período de 60 (sessenta) dias, duas ocorrências de defeitos por inoperância ou três ocorrências de deficiência operacional que comprometam o funcionamento regular da solução.

Todas as ferramentas, recursos técnicos, atualizações e demais meios necessários à manutenção da solução serão de inteira responsabilidade da contratada, sem ônus adicional para a contratante.

1.3.3.4. Requisitos de Projeto e de Implementação:

A CONTRATADA deverá apresentar plano de projeto contemplando cronograma, etapas de execução, responsabilidades, marcos de entrega e metodologia de implementação da solução.

O projeto deverá prever, no mínimo, as fases de planejamento, instalação, configuração, parametrização, testes, validação e entrada em produção.

Deverá ser designado responsável técnico pela CONTRATADA para condução do projeto, atuando como ponto focal junto à equipe técnica do PJAC.

A implementação deverá observar boas práticas de segurança da informação e de gestão de mudanças, garantindo rastreabilidade das configurações realizadas e registro formal das atividades executadas.

A CONTRATADA deverá fornecer documentação técnica completa da solução implementada, incluindo arquitetura adotada, políticas configuradas, integrações realizadas e procedimentos operacionais básicos.

Quaisquer ajustes de configuração necessários para adequação ao ambiente do PJAC deverão estar contemplados no escopo do projeto, sem ônus adicional.

1.3.3.5. Requisitos de Implantação:

A implantação da solução deverá ocorrer de forma planejada e controlada, minimizando impactos aos serviços em produção e à operação regular do PJAC.

A solução deverá ser instalada e configurada no ambiente institucional, contemplando a instalação de agentes nos endpoints definidos, parametrização inicial de políticas de segurança e integração com demais ferramentas existentes, quando aplicável.

Deverão ser realizados testes de funcionamento e validação técnica antes da entrada definitiva em produção, garantindo que a solução esteja operando conforme os requisitos estabelecidos.

A implantação deverá contemplar a cobertura integral do quantitativo contratado de endpoints, podendo ser realizada de forma gradual, mediante cronograma acordado entre as partes.

A entrada em produção somente ocorrerá após validação formal da CONTRATANTE, com emissão do respectivo Termo de Recebimento.

1.3.3.6. Requisitos de Experiência Profissional:

A CONTRATADA deverá disponibilizar equipe técnica qualificada para execução dos serviços de instalação, configuração, parametrização, suporte e repasse de conhecimento da solução de segurança de endpoints com XDR.

Os profissionais envolvidos na implementação e suporte da solução deverão possuir conhecimento técnico na tecnologia ofertada, poderão ser solicitados certificação oficial do fabricante ou comprovação de capacitação técnica equivalente.

A equipe técnica deverá possuir capacidade para atuar na análise de incidentes, parametrização de políticas de segurança, integração da solução ao ambiente existente e orientação técnica à equipe interna do PJAC.

Os requisitos de experiência profissional visam assegurar a adequada execução do objeto contratual, mitigando riscos técnicos e garantindo a correta implantação e operação da solução no ambiente institucional.

1.3.3.7. Requisitos de Formação da Equipe:

A CONTRATADA deverá disponibilizar equipe técnica com formação compatível com a natureza e complexidade da solução de segurança a ser implantada no PJAC.

Os profissionais responsáveis pela implementação, configuração e suporte da solução deverão possuir formação técnica ou superior na área de Tecnologia da Informação ou áreas afins, compatível com as atividades a serem desempenhadas.

1.3.3.8. Requisitos Temporais:

O início da execução do objeto ocorrerá em até 30 (trinta) dias corridos, contados da assinatura do contrato, podendo ser antecipado mediante comum acordo entre as partes e formalização por meio de Ordem

de Serviço.

A solução deverá ser implantada integralmente em até 90 (noventa) dias corridos, contados da emissão da Ordem de Serviço, observando-se a necessidade de garantir a continuidade dos serviços em produção e mitigar riscos de indisponibilidade, conforme às seguintes fases:

Evento	Descrição	Prazo em dias	Responsável
1	Assinatura do contrato		Contratada e Contratante
2	Reunião inicial	Evento 1 + 5 dias úteis	Contratada e Contratante
3	Entrega do Plano de Implantação	Evento 2 + 10 dias úteis	Contratada
4	Aprovação do Plano de Implantação	Evento 3 + 5 dias úteis	Contratante
5	Repasse de Conhecimento	Evento 4 + 10 dias úteis	Contratada
6	Recebimento Provisório do Repasse de Conhecimento	Evento 5 + 5 dias úteis	Contratante
7	Entrega do Software e Licenças com Suporte de Direito de Atualização	Evento 5 + 5 dias úteis	Contratada
8	Implantação	Evento 5 + 20 dias úteis	Contratada
9	Recebimento Provisório do Software com as Licenças e a Implantação	Evento 8 + 5 dias úteis	Contratante
10	Recebimento Definitivo	Evento 9 + 10 dias úteis	Contratante

A entrega das informações referentes ao suporte técnico e ao direito de atualização da solução deverá incluir:

Comprovação formal do registro do suporte junto ao fabricante, pelo período total contratado;

- Informações necessárias para utilização do suporte e direito de atualização do produto
- Dados necessários para utilização do direito de atualização e download de versões, patches e correções disponibilizadas pelo fabricante.

1.3.3.9. Requisitos de Segurança da Informação:

A CONTRATADA deverá observar integralmente os regulamentos, normas e instruções de Segurança da Informação e Comunicações adotados pelo Poder Judiciário do Estado do Acre (PJAC), incluindo a Política de Segurança da Informação e suas normas complementares, durante toda a execução contratual.

A CONTRATADA deverá garantir a disponibilidade, integridade, confidencialidade, autenticidade e sigilo das informações, documentos e dados aos quais tiver acesso em razão da execução do contrato, responsabilizando-se por eventuais perdas, danos ou uso indevido que venham a ocorrer por ação ou omissão de seus profissionais.

Toda informação confidencial gerada, acessada ou manipulada em decorrência do contrato, independentemente do meio de armazenamento (físico, magnético ou eletrônico), deverá ser devolvida ou eliminada, mediante formalização entre as partes, nas seguintes hipóteses:

a) término ou rescisão contratual;

b) solicitação formal da CONTRATANTE.

A CONTRATADA deverá utilizar ferramentas, mecanismos e controles adequados de proteção da informação, de modo a impedir acesso não autorizado, vazamento de dados ou comprometimento dos sistemas e softwares utilizados na execução do objeto.

Quando formalmente solicitado pela CONTRATANTE, a CONTRATADA deverá priorizar e realizar ajustes necessários para correção de vulnerabilidades, falhas de segurança ou configurações que representem risco ao ambiente institucional.

A CONTRATADA deverá comunicar formalmente à CONTRATANTE quaisquer necessidades de atualização, alteração de configuração ou medidas corretivas que impactem a segurança da solução ou do ambiente.

É obrigação da CONTRATADA prestar esclarecimentos técnicos e fornecer informações detalhadas sobre a execução dos serviços, sempre que solicitado pela CONTRATANTE.

A CONTRATADA deverá garantir a integridade e disponibilidade das informações sob sua guarda, respondendo por eventuais danos decorrentes de falhas na execução contratual.

É vedada à CONTRATADA a divulgação, reprodução ou utilização de informações obtidas em razão do contrato, mesmo que em caráter estatístico, sem autorização prévia e formal da CONTRATANTE.

O acesso às instalações da CONTRATANTE, quando necessário, deverá ser controlado e restrito a profissionais autorizados, devidamente identificados. A CONTRATADA deverá substituir imediatamente qualquer profissional que descumpra normas disciplinares ou comprometa a segurança do ambiente institucional.

A CONTRATADA deverá assegurar que seus profissionais tenham pleno conhecimento das normas de segurança e disciplina da CONTRATANTE, exigindo sua fiel observância durante toda a execução contratual.

A CONTRATADA deverá manter sigilo absoluto sobre todas as informações, documentos, dados e registros aos quais tiver acesso em decorrência da execução do contrato.

1.3.3.10. Requisitos Sociais, Ambientais e Culturais:

A CONTRATADA deverá observar diretrizes de responsabilidade social, ambiental e cultural durante a execução do objeto contratual, em conformidade com as políticas institucionais do PJAC e com as boas práticas de sustentabilidade na Administração Pública.

A execução dos serviços deverá priorizar o uso racional de recursos, evitando desperdício de materiais, energia e insumos, bem como a geração desnecessária de resíduos, em consonância com as diretrizes de sustentabilidade adotadas pelo PJAC.

A CONTRATADA deverá orientar seus profissionais quanto à importância da racionalização de recursos, redução de consumo, reutilização de materiais e descarte ambientalmente adequado de resíduos eventualmente gerados no desempenho das atividades.

A empresa deverá permitir e incentivar a participação de seus colaboradores em ações, eventos ou campanhas de capacitação e sensibilização promovidas pela CONTRATANTE, voltadas à sustentabilidade, responsabilidade ambiental e boas práticas institucionais.

Estes requisitos visam assegurar que a contratação esteja alinhada aos princípios da responsabilidade socioambiental e às políticas públicas de sustentabilidade aplicáveis à Administração Pública.

1.3.3.11. Requisitos Legais:

O presente processo de contratação deverá observar e estar em conformidade com a legislação vigente aplicável à Administração Pública e às contratações de Tecnologia da Informação e Comunicação.

A contratação deverá estar aderente à:

- Constituição Federal de 1988;
- Lei nº 14.133/2021 (Lei de Licitações e Contratos Administrativos);
- Resolução CNJ nº 468/2022, que dispõe sobre a governança e gestão de contratações de TIC no âmbito do Poder Judiciário;

- Resolução CNJ nº 396/2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);
- Instrução Normativa SGD/ME nº 94/2022, no que couber;
- Instrução Normativa SEGES/ME nº 65/2021, no que couber;
- Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD);
- Demais normas internas do PJAC relacionadas à segurança da informação, governança de TIC e gestão contratual.

A solução contratada deverá atender às exigências legais relativas à proteção de dados pessoais, segurança da informação e continuidade dos serviços públicos digitais, garantindo conformidade normativa durante toda a vigência contratual.

1.3.3.12. Demais Requisitos Aplicáveis:

- Garantir prazos de entrega a fim de evitar penalidades por atrasos;
- Desenvolver as atividades necessárias mediante trabalho híbrido (remoto/presencial) e nos termos dos padrões de segurança e integridade previstas pelo Poder Judiciário e pelo CNJ;
- A CONTRATADA deverá estar apta a abrir e receber Ordens de Serviço via correio eletrônico, sistema específico de controle de demandas ou, página na internet (WEB) dedicada, em regime 24x7 (24 horas por dia, em todos os sete dias da semana);
- Responsabilizar-se pelos materiais, produtos, ferramentas, instrumentos e equipamentos disponibilizados para a execução dos serviços, sejam eles prestados remotamente ou nas instalações do PJAC, não cabendo ao PJAC qualquer responsabilidade por perdas decorrentes de roubo, furto ou outros fatos que possam vir a ocorrer;
- Promover o afastamento, no prazo máximo de 24 (vinte e quatro) horas após o recebimento da notificação por ofício ou e-mail, de qualquer dos seus recursos técnicos que não correspondam aos critérios de confiança ou que perturbem a ação da equipe de fiscalização do PJAC;
- Garantir a execução e sustentação dos padrões de qualidade na geração dos produtos e soluções associados ao provimento da Solução XDR.

1.3.4. Aderência a padrões e modelos

Considerando que o objeto da contratação consiste em solução de proteção de endpoints (XDR), não se aplica diretamente a padrões relacionados à interoperabilidade entre sistemas governamentais (MNI/e-PING), certificação digital (ICP-Brasil) ou gestão arquivística de documentos digitais (MoReq-Jus).

1.3.4.1. Modelo Nacional de Interoperabilidade - MNI

Não se aplica.

1.3.4.2. Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil

Não se aplica.

1.3.4.1. Modelo de Requisitos MoReq-Jus

Não se aplica.

1.4. Atendimento da demanda

1.4.1. Portal do Software Público Brasileiro

Em atendimento aos princípios da economicidade, eficiência e busca por soluções tecnicamente adequadas e potencialmente menos onerosas, foi realizada consulta ao Portal do Software Público Brasileiro (SPB), com o objetivo de verificar a existência de solução capaz de atender aos requisitos estabelecidos para proteção avançada de endpoints no âmbito do PJAC.

A análise técnica considerou os seguintes requisitos mínimos definidos para a presente demanda: Capacidade de Detecção e Resposta; Monitoramento contínuo e centralizado de aproximadamente 2.700 endpoints; Análise comportamental baseada em machine learning; Correlação de eventos em tempo real; Resposta automatizada a incidentes (isolamento, bloqueio, contenção); Inteligência de ameaças atualizada continuamente; Mitigação de ataques avançados (ransomware, fileless, zero-day, movimentação lateral); Escalabilidade e integração com outras camadas de segurança; Suporte técnico especializado e atualização contínua da solução.

As soluções disponibilizadas no Portal do Software Público Brasileiro não contemplam arquitetura corporativa, mecanismos avançados de detecção comportamental com inteligência global de ameaças, nem modelo estruturado de suporte técnico com atualizações contínuas de assinaturas, heurísticas e mecanismos de defesa.

Adicionalmente, considerando a criticidade dos serviços judiciais suportados pela infraestrutura tecnológica do PJAC, bem como a necessidade de proteção contra ameaças sofisticadas e em constante evolução, conclui-se que a adoção de solução baseada exclusivamente em software público não atenderia aos níveis de segurança, disponibilidade e resposta exigidos para o contexto institucional.

Dessa forma, não se verificou viabilidade técnica para utilização de solução proveniente do Portal do Software Público Brasileiro para atendimento da presente demanda, sendo necessária a contratação de solução especializada de mercado, com características compatíveis com o porte, a criticidade e o nível de exposição a riscos do ambiente do PJAC.

1.4.2. Soluções de TIC

Foi realizada análise comparativa entre alternativas tecnológicas capazes de atender à necessidade de proteção de endpoints do PJAC, considerando aspectos técnicos, econômicos e qualitativos, bem como soluções adotadas por outros órgãos da Administração Pública.

A análise contemplou a aquisição de solução de Detecção e Resposta Estendida (XDR) e a manutenção da solução atualmente utilizada, baseada em antivírus tradicional.

1.4.2.1. Solução 1: Aquisição de solução de segurança abrangente para proteção de endpoints e defesa contra ataques avançados

A solução consiste na aquisição de ferramenta de segurança abrangente voltada à proteção de estações de trabalho e servidores do PJAC, com capacidade de prevenção, detecção, análise e resposta a ameaças cibernéticas avançadas.

A contratação engloba o fornecimento de licenciamento da solução para aproximadamente 2.700 endpoints, bem como os serviços de instalação, configuração, parametrização, transferência de conhecimento, suporte técnico especializado e garantia de atualização, pelo período de 24 (vinte e quatro) meses.

Sob o aspecto econômico, embora represente investimento superior à manutenção de antivírus tradicional, a solução apresenta melhor relação custo-benefício quando considerados os riscos associados à indisponibilidade de sistemas judiciais, vazamento de dados sensíveis e paralisação de atividades essenciais à prestação jurisdicional.

Sob o aspecto qualitativo, a solução promove elevação do nível de maturidade em segurança da informação do PJAC, maior visibilidade sobre o ambiente tecnológico, redução do tempo de detecção e

resposta a incidentes e maior aderência às diretrizes de segurança estabelecidas pelo Conselho Nacional de Justiça.

Considerando a criticidade dos serviços suportados e o aumento da sofisticação das ameaças cibernéticas direcionadas ao setor público, a solução mostra-se tecnicamente adequada para atendimento às necessidades institucionais ao longo do período contratual de 24 meses.

1.4.2.2. Solução 2: Manutenção da ferramenta atual (antivírus tradicional)

A alternativa consiste na manutenção da solução atualmente utilizada, baseada em antivírus tradicional por assinaturas.

Sob o aspecto econômico, essa alternativa apresenta custo inicial inferior, uma vez que mantém modelo já contratado e com menor complexidade tecnológica.

Entretanto, sob o aspecto qualitativo e técnico, a solução apresenta limitações relevantes:

- Dependência predominante de assinaturas de ameaças conhecidas;
- Ausência de análise comportamental avançada;
- Inexistência de mecanismos estruturados de resposta automatizada;
- Baixa visibilidade sobre movimentação lateral e ataques sofisticados;
- Cobertura insuficiente frente ao crescimento do parque computacional (2.700 endpoints).

A manutenção da solução atual não atende plenamente às necessidades de segurança identificadas, tampouco acompanha a evolução do cenário de ameaças cibernéticas, podendo expor o PJAC a riscos operacionais significativos.

Além disso, essa alternativa não contribui para a elevação do nível de maturidade em segurança exigido pelas diretrizes do CNJ e pelas boas práticas de governança de TIC no Poder Judiciário.

1.4.3. Contratações Públicas Similares

1.4.3.1. Órgão 1: Secretaria de Administração do Estado do Piauí (SEAD-PI)

O órgão realizou a transição tecnológica para a plataforma Trend Micro Vision One, caracterizada como XDR Nativo. A escolha técnica pautou-se na necessidade de correlação de eventos entre endpoints, servidores e rede, permitindo a detecção de ameaças furtivas e o uso de Inteligência Artificial para resposta orquestrada a incidentes. A contratação inclui suporte proativo e repasse de conhecimento certificado, através do Pregão Eletrônico nº 12/2025/SEAD.
Solução Adotada: Solução 1.

1.4.3.2. Órgão 2: Universidade Federal do Rio Grande do Sul (UFRGS)

A instituição realizou a cessão de direitos de uso da solução Kaspersky Endpoint Security NEXT EDR OPTIMUM. A especificação técnica exigiu capacidades de análise comportamental e telemetria estendida, visando proteger um ambiente acadêmico distribuído contra movimentações laterais e exploits de dia zero, reforçando a inviabilidade técnica da manutenção de ferramentas tradicionais (Solução 2), através da do Pregão Eletrônico nº 90326/2025 (UASG: 153114).

1.4.3.2. Órgão 3: Município de Jaboticabal/SP

O órgão optou pela renovação tecnológica através do software Kaspersky Next EDR Optimum. A justificativa técnica baseou-se na superação das limitações do antivírus comum, adotando uma camada de Detecção e Resposta (EDR) que permite a investigação de causa raiz e a visibilidade de vetores de ataque complexos, características ausentes na Solução 2, através do Pregão Eletrônico nº 000394/2025 (ID PNCP: 50387844000105-1-000394/2025).

1.4.4. Soluções similares em outros órgãos

A análise técnico-comparativa demonstra uma clara tendência de descontinuidade da Solução 2 (Antivírus Tradicional) em ambientes de alta criticidade. A pesquisa em portais oficiais, como o Compras.gov.br e o PNCP, revela que órgãos como a Prefeitura de São Francisco de Paula/RS (Pregão nº 000118/2025) também aderiram à Solução 1, especificando licenças de Kaspersky Next EDR com suporte técnico especializado por 36 meses.

Tecnicamente, a convergência para o XDR/EDR justifica-se pela incapacidade do modelo tradicional em lidar com ataques fileless (sem arquivo) e o aumento do tempo médio de resposta (MTTR) em ferramentas sem automação. Enquanto a Solução 2 limita-se ao bloqueio de binários conhecidos, a Solução 1 — exemplificada pelas tecnologias Trend Micro Vision One e Kaspersky Next observadas no mercado — oferece Virtual Patching, análise de comportamento de processos e correlação de telemetria, atendendo integralmente às diretrizes de segurança cibernética do Poder Judiciário estabelecidas na Resolução CNJ nº 396/2021.

1.4.5. Modelos de Aquisição/Prestação do Serviço

A análise dos modelos de prestação do serviço indicou que a Solução 1 é predominantemente ofertada no mercado de TIC sob o modelo de Software como Serviço (SaaS - Software as a Service), com gerenciamento centralizado em nuvem do fabricante. Este modelo apresenta-se superior à aquisição na forma de bens (licenciamento perpétuo), pois garante a atualização tecnológica contínua (corretiva, adaptativa e evolutiva) e o acesso imediato a bases de inteligência de ameaças em tempo real, sem necessidade de investimentos vultosos em infraestrutura local de hardware. No que tange à possibilidade de ampliação ou substituição, a contratação visa a substituição integral da solução de antivírus tradicional (Solução 2) por uma plataforma de XDR, permitindo a escalabilidade do licenciamento conforme o crescimento do parque tecnológico do Poder Judiciário. As métricas de prestação do serviço e de pagamento foram definidas com base na unidade de medida por dispositivo (endpoint) e por servidor protegido, o que assegura um faturamento vinculado ao consumo real e à efetiva disponibilidade das licenças e serviços de suporte. Adicionalmente, os serviços de implantação, suporte proativo e capacitação são mensurados por solução ou carga horária, garantindo a aferição objetiva da execução contratual antes da liquidação financeira.

1.4.6. Capacidade e alternativas do mercado de TIC

A pesquisa de mercado demonstrou que o setor privado de TIC possui alta maturidade e capacidade para fornecer a Solução 1, com diversos fabricantes globais consolidados em quadrantes de liderança tecnológica e com vasta experiência no setor público. Entre os principais fornecedores identificados em análises de mercado e contratações similares, destacam-se a a Kaspersky, Trend Micro, CrowdStrike, Palo Alto Networks e Check Point. Esses fabricantes oferecem arquiteturas de XDR/EDR que atendem aos requisitos de detecção baseada em Inteligência Artificial, análise comportamental e resposta automatizada exigidos por este Tribunal.

Quanto à existência de software livre ou público, verificou-se que, embora o Portal do Software Público Brasileiro estimule o compartilhamento de soluções, não foram identificadas ferramentas que atendam à natureza crítica da demanda. Soluções de código aberto para segurança de endpoints exigem alta complexidade de integração manual de múltiplos produtos e carecem de suporte técnico especializado 24x7 e Acordos de Nível de Serviço (SLA) garantidos por contrato, o que elevaria o risco de vulnerabilidades e comprometeria a conformidade com as diretrizes de segurança do CNJ. Assim, a contratação via mercado privado ou adesão a atas vigentes mostra-se a única alternativa capaz de assegurar a resiliência cibernética necessária à prestação jurisdicional.

1.4.7. Contratações correlatas e/ou interdependentes

A análise das necessidades de segurança cibernética do Tribunal de Justiça do Estado do Acre (PJAC) revela que qualquer que seja a alternativa técnica adotada (Solução 1 ou Solução 2), sua execução guardará estrita correlação e interdependência com processos de contratação já em andamento para o exercício de 2026. A integração entre esses diferentes ativos é essencial para a manutenção da disponibilidade dos serviços jurisdicionais e o cumprimento da Estratégia Nacional de Segurança Cibernética do Poder Judiciário.

Verificou-se interdependência técnica com o processo 2025-206 (Serviço de instalação e configuração da solução PAM – Privileged Access Management). Independentemente da tecnologia de proteção de endpoint escolhida, esta deverá coexistir e interoperar com a gestão de acessos privilegiados, visando garantir que o monitoramento de dispositivos finais auxilie na identificação de tentativas de uso indevido de credenciais administrativas, fortalecendo o controle sobre contas críticas da instituição.

Adicionalmente, identifica-se correlação com o processo 2025-415 (Centro de Operações de Segurança – SOC). A solução de proteção de endpoints (seja via XDR ou antivírus tradicional) funcionará como uma das diversas fontes de telemetria a serem integradas ao SOC. Os logs e alertas gerados nos dispositivos clientes e servidores alimentarão o fluxo de monitoramento contínuo e resposta estruturada a incidentes, permitindo que a equipe do SOC analise os eventos de endpoint de forma contextualizada com as demais camadas de segurança do Tribunal.

Por fim, há correlação com o processo 2025-442 (Serviços de Centro de Operações de Rede – NOC 24x7). A visibilidade da infraestrutura de rede provida pelo NOC deve estar alinhada ao estado de saúde e segurança dos endpoints. A comunicação ininterrupta entre as equipes de operações de rede e os dados provenientes da solução de segurança de endpoints será vital para a triagem de falhas operacionais e a rápida identificação de incidentes que possam comprometer a estabilidade do parque tecnológico composto por aproximadamente 2.700 equipamentos.

1.5. Análise dos Custos Totais da Demanda

Item	Soluções identificadas	Especificação	CATMAT CATSER	Qtd	Órgão(s) que adotaram a solução	Vantagens e Benefícios	Desvantagens e riscos	Custo(s) envolvido(s)
1	Solução 1	Solução de proteção de Endpoints e Servidores com abordagem proativa para resposta eficaz a incidentes; serviços de implantação, suporte proativo/corretivo e capacitação/repasse de conhecimento.	XXX	2500	UFRGS, SEAD-PI e Município de Jaboticabal	Proteção contra ataques avançados, correlação de eventos, resposta automatizada e conformidade com a Resolução CNJ nº 396/2021	Necessidade de investimento de maior volume para modernização da arquitetura de segurança.	Preço unitário médio de R$ 300,40; Acrescido de: Suporte 24x7, Serviço de implantação e Serviço de capacitação.

1.6.1. Descrição da Solução Escolhida

A solução a ser contratada consiste na aquisição de plataforma integrada de segurança para proteção de endpoints e cargas de trabalho híbridas, com capacidades avançadas de detecção e resposta a incidentes, disponibilizada na modalidade de serviço (SaaS), com gerenciamento centralizado em nuvem do fabricante.

A solução abrangerá aproximadamente 2.700 equipamentos, entre estações de trabalho e servidores, atendendo cerca de 2.100 usuários ativos do Poder Judiciário do Estado do Acre, incluindo magistrados, servidores e colaboradores.

Características do serviço e da solução

Solução de Proteção de Endpoints com Abordagem Proativa para Resposta Eficaz a Incidentes

A solução visa oferecer uma camada robusta de defesa para os endpoints da rede institucional, incluindo estações de trabalho e dispositivos corporativos, com foco na prevenção, detecção e resposta a ameaças cibernéticas.

A proteção contempla mecanismos avançados contra malware, ransomware, vírus e outras ameaças modernas, incorporando tecnologias como firewall de host, antivírus/antimalware, detecção e bloqueio de intrusões, controle de aplicações, controle de dispositivos, análise comportamental e recursos de detecção e resposta a incidentes.

A solução é essencial para garantir a integridade, confidencialidade e disponibilidade dos dispositivos e dos dados neles armazenados, especialmente em ambiente corporativo crítico como o do Poder Judiciário, onde a proteção dos endpoints é componente fundamental da segurança global da infraestrutura tecnológica.

Solução de Proteção de Servidores com Abordagem Proativa para Resposta Eficaz a Incidentes

A proteção de servidores constitui elemento estratégico da segurança da informação institucional, considerando que esses ativos armazenam, processam e disponibilizam dados críticos e sensíveis, além de hospedarem sistemas judiciais, bancos de dados e serviços essenciais ao funcionamento do órgão.

A solução deverá prover mecanismos de prevenção, detecção e resposta a ataques direcionados a servidores físicos, virtuais ou em ambientes híbridos, incluindo proteção contra exploração de vulnerabilidades, ataques a aplicações web, movimentação lateral, ransomware e demais ameaças avançadas.

Essa camada de proteção fortalece a resiliência da infraestrutura tecnológica, reduzindo riscos de indisponibilidade, vazamento de dados e comprometimento de serviços essenciais à prestação jurisdicional.

Serviço de Suporte Proativo, Corretivo e Resposta a Incidentes

O serviço de suporte abrange atuação preventiva, corretiva e reativa, com o objetivo de: Antecipar e mitigar riscos por meio de acompanhamento técnico; Corrigir falhas ou inconsistências identificadas no ambiente e Responder de forma rápida e estruturada a incidentes de segurança.

O suporte inclui atualização contínua da solução, aplicação de correções, orientação técnica especializada e apoio à investigação e contenção de incidentes, contribuindo para a manutenção da estabilidade, disponibilidade e segurança do ambiente tecnológico.

Serviço de Implantação

O serviço de implantação compreende suporte técnico especializado para implementação da solução de segurança no ambiente corporativo do PJAC.

Inclui planejamento, configuração inicial, parametrização de políticas, instalação e ativação de agentes, integração com a infraestrutura existente e validação operacional, assegurando que a solução seja implementada de forma eficiente, segura e alinhada às necessidades institucionais.

Serviço de Capacitação e Repasse de Conhecimento

O serviço de capacitação visa promover a transferência de conhecimento técnico à equipe da contratante, garantindo autonomia operacional na administração, monitoramento e resposta a incidentes relacionados à solução contratada.

A capacitação permitirá que os profissionais adquiram habilidades para operar, configurar, gerenciar e manter a solução de forma adequada, assegurando o aproveitamento pleno de suas funcionalidades e contribuindo para o fortalecimento da maturidade em segurança cibernética institucional.

Motivação e Justificativa da Escolha

A escolha da solução de proteção de endpoints e cargas de trabalho híbridas com abordagem proativa de detecção e resposta a incidentes fundamenta-se em critérios técnicos, operacionais, estratégicos e

econômicos, considerando o porte do ambiente do Poder Judiciário do Estado do Acre e o atual cenário de ameaças cibernéticas direcionadas ao setor público.

O ambiente tecnológico do PJAC é composto por aproximadamente 2.700 equipamentos, entre estações de trabalho e servidores, que suportam sistemas judiciais eletrônicos, bancos de dados processuais, serviços administrativos e canais digitais de atendimento ao jurisdicionado. A indisponibilidade ou comprometimento desses ativos impacta diretamente a continuidade da prestação jurisdicional e o direito fundamental de acesso à Justiça.

A solução atualmente utilizada, baseada em antivírus tradicional, apresenta limitações técnicas relevantes, especialmente quanto à: Ausência de análise comportamental avançada;

Incapacidade de correlação de eventos; Baixa visibilidade contextual de ataques; Limitação na resposta automatizada a incidentes; Insuficiência frente ao quantitativo atualizado de ativos tecnológicos.

Diante do aumento da sofisticação dos ataques cibernéticos — especialmente ransomware, exploração de vulnerabilidades, movimentação lateral e uso indevido de credenciais — torna-se necessária a adoção de solução mais abrangente, capaz de atuar de forma preventiva, detectiva e responsiva.

A alternativa escolhida demonstra-se mais vantajosa para a Administração pelos seguintes aspectos:

Eficácia

Elevação significativa da capacidade de prevenção, detecção e contenção de ameaças conhecidas e desconhecidas;

Redução do tempo médio de detecção e resposta (MTTD e MTTR);

Maior visibilidade sobre comportamentos anômalos nos endpoints e servidores.

Eficiência

Gestão centralizada em console única;

Automação de políticas e ações de contenção;

Redução de esforço operacional da equipe de TIC;

Integração com outras camadas de segurança, preparando o ambiente para futura estruturação de SOC.

Efetividade

Fortalecimento da resiliência institucional;

Mitigação de riscos de indisponibilidade dos sistemas judiciais;

Proteção de dados sensíveis e informações processuais;

Preservação da confiança do jurisdicionado nos serviços digitais do Tribunal.

Economicidade

A mitigação de impactos operacionais e reputacionais;

A previsibilidade orçamentária com suporte e atualização por 24 meses.

A alternativa de manutenção da solução atual não atende às necessidades técnicas identificadas, ampliando o risco institucional e contrariando as boas práticas de segurança cibernética exigidas para o Poder Judiciário.

Declaração de Viabilidade da Contratação

Com base na análise técnica, mercadológica e institucional realizada no presente Estudo Técnico Preliminar, declara-se viável a contratação da solução de segurança para proteção de endpoints e cargas de trabalho híbridas, considerando que:

- Atende plenamente ao quantitativo e à complexidade do ambiente tecnológico do PJAC;
- Está alinhada às diretrizes nacionais de segurança cibernética aplicáveis ao Poder Judiciário;
- Contribui diretamente para a continuidade da prestação jurisdicional;
- Possui aderência às boas práticas de mercado em segurança da informação;
- Inclui implantação, capacitação, suporte técnico e direito de atualização durante todo o período contratual;
- Apresenta benefícios superiores em termos de eficácia, eficiência, efetividade e economicidade quando comparada à alternativa de manutenção da solução atualmente utilizada.

Dessa forma, conclui-se que a contratação é tecnicamente adequada, operacionalmente necessária e economicamente justificável, representando a alternativa mais vantajosa para a Administração Pública no

contexto do Poder Judiciário do Estado do Acre.

1.6.2. Benefícios Esperados

A contratação da solução de proteção de endpoints e cargas de trabalho híbridas proporcionará benefícios institucionais relevantes ao PJAC, especialmente sob os aspectos de eficácia, eficiência, economicidade e padronização.

Eficácia: Ampliação da capacidade de prevenção, detecção e resposta a incidentes cibernéticos, reduzindo riscos de indisponibilidade dos sistemas judiciais e de comprometimento de dados sensíveis.

Eficiência: Gestão centralizada e automatizada dos ativos tecnológicos, com redução de atividades manuais repetitivas e melhor aproveitamento da equipe de TIC, permitindo foco em ações estratégicas.

Economicidade: Mitigação de custos decorrentes de incidentes de segurança, redução de retrabalho técnico e maior previsibilidade orçamentária, além de economia potencial com a correção preventiva de vulnerabilidades e potenciais irregularidades.

Padronização: Uniformização das políticas e controles de segurança, consolidação tecnológica em plataforma única e melhoria da governança e rastreabilidade de eventos.

Aspectos Qualitativos: Economia potencial com a correção tempestiva de potenciais irregularidades relacionadas à segurança da informação; Resolução de irregularidades não diretamente associadas a pagamentos, mediante adoção de medidas corretivas estruturadas; Utilização de menor força de trabalho operacional em razão da automatização dos serviços; Maior agilidade e segurança na execução de políticas institucionais, inclusive aquelas relacionadas à gestão de usuários e acessos.

A solução contribuirá diretamente para a continuidade da prestação jurisdicional e para o fortalecimento da maturidade em segurança cibernética do PJAC.

1.6.3. Resultados Esperados

Em conformidade com o §1º, inciso IX, do art. 18 da Lei nº 14.133/2021, a contratação visa alcançar resultados concretos em termos de economicidade e melhor aproveitamento dos recursos humanos, materiais e financeiros disponíveis.

Espera-se como resultados principais:

- Redução mensurável do número de incidentes de segurança com impacto operacional;
- Diminuição do tempo médio de detecção e resposta a incidentes;
- Maior disponibilidade dos sistemas judiciais;
- Redução de custos indiretos associados à recuperação de ambientes comprometidos;
- Melhor aproveitamento da equipe técnica, com foco em atividades estratégicas e preventivas;
- Otimização do uso dos recursos tecnológicos já existentes, por meio de integração e centralização da gestão de segurança.

A solução permitirá maior previsibilidade orçamentária, redução de riscos institucionais e melhor aproveitamento dos investimentos realizados em infraestrutura tecnológica, contribuindo para o fortalecimento da governança de TIC no PJAC.

Conclui-se que os resultados pretendidos estão alinhados aos princípios da eficiência, economicidade e interesse público, demonstrando que a contratação representa medida estratégica e sustentável para a proteção do ambiente tecnológico institucional.

1.6.4. Relação entre a Demanda Prevista e a quantidade de bens e/ou serviços Contratados

O dimensionamento da contratação foi realizado com base no levantamento atualizado do parque tecnológico do Poder Judiciário do Estado do Acre, considerando dados extraídos do Wazuh e do servidor de antivírus atualmente em operação.

O ambiente institucional atualmente é composto por:

2.031 estações de trabalho em operação;

150 novos computadores adquiridos por meio do Processo nº 2025-410;

99 servidores classificados como críticos, responsáveis por hospedar sistemas judiciais, bancos de dados e serviços essenciais.

Item 1 – Licenciamento Padrão (Perfil Endpoint):

2.031 estações atualmente em operação;

150 novas estações adquiridas.

Total base do Item 1: 2.031 + 150 = 2.181 licenças

Aplicando crescimento planejado de 10%: 2.181 × 10% = 218 licenças adicionais (aproximadamente)

Total estimado do Item 1: 2.181 + 218 2.399 licenças

Assim vamos arredondar tecnicamente para 2.400 para facilitar a gestão contratual.

Item 2 – Licenciamento para Servidores Críticos (Proteção Reforçada) inclui:

90 servidores classificados como críticos, responsáveis por hospedar sistemas judiciais, bancos de dados e serviços essenciais.

Aplicando margem técnica de crescimento de 10%: 90 × 10% = 9 licenças adicionais.

Total estimado do Item 2: 90 + 9 = 99 licenças

Assim vamos arredondar tecnicamente para 100 licenças para facilitar a gestão contratual.

Justificativa do Dimensionamento

A aplicação da margem técnica observa o crescimento vegetativo da infraestrutura e a necessidade de continuidade da proteção reforçada para ativos de alta criticidade, evitando insuficiência de licenciamento ao longo da execução contratual.

A separação dos itens por criticidade demonstra planejamento técnico baseado em análise de risco, assegurando proporcionalidade da contratação, aderência ao princípio da eficiência e adequada gestão dos recursos públicos.

Item	Descrição	CATSER	Unidade	Qtd Unitária	Qtd total
1	Solução de proteção de Endpoints com abordagem proativa para resposta eficaz a incidentes		Por Endpoint	Endpoint	2400
2	Solução de proteção de Servidores com abordagem proativa para resposta eficaz a incidentes.		Por Servidor	Servidor	100
3	Serviço de suporte proativo, corretivo e para resposta a incidentes		Por Solução	Solução	2
4	Serviço de implantação		Por Solução	Solução	2
5	Serviço de capacitação e repasse de conhecimento		40 Horas	40 Horas	1

1.6.5. Estimativa do Custo Total da Solução Escolhida

Item	Descrição	Unidade	Qtd	Valor Unitário	Valor total

1	Solução de proteção de Endpoints com abordagem proativa para resposta eficaz a incidentes	Por Endpoint	2400	R$ 292,00	R$ 759.200,00
2	Solução de proteção de Servidores com abordagem proativa para resposta eficaz a incidentes	Por Servidor	100	R$ 2.475,25	R$ 247.525,00
3	Serviço de suporte proativo, corretivo e para resposta a incidentes	Por Solução	2	R$ 109.974,71	R$ 219.949,42
4	Serviço de implantação	Por Solução	2	R$ 22.850,43	R$ 45.700,86
5	Serviço de capacitação e repasse de conhecimento	40 Horas	1	R$ 21.750,00	R$ 21.750,00

1.7. Declaração de viabilidade da contratação

1.7.1. Declaração de Viabilidade:

(X) Viável;

(   ) Viável com restrições;

(   ) Inviável.

Com base nas análises técnicas, operacionais e de mercado realizadas no âmbito deste Estudo Técnico Preliminar, a Equipe de Planejamento da Contratação conclui pela viabilidade da contratação da solução de segurança para proteção de endpoints e servidores, considerando sua aderência às necessidades institucionais do Poder Judiciário do Estado do Acre.

Os estudos realizados demonstraram que a solução proposta atende aos requisitos funcionais, técnicos, operacionais e de segurança da informação definidos para o ambiente tecnológico institucional, contribuindo para o fortalecimento da postura de segurança cibernética, mitigação de riscos e aumento da capacidade de detecção e resposta a incidentes de segurança.

Adicionalmente, verificou-se que a contratação apresenta relação custo-benefício adequada, alinhamento com práticas modernas de proteção de ambientes corporativos e aderência às diretrizes normativas aplicáveis à Administração Pública, incluindo a Lei nº 14.133/2021, a Resolução CNJ nº 468/2022 e demais normativos relacionados à governança e segurança da informação.

Dessa forma, conclui-se que a contratação é tecnicamente e economicamente viável, contribuindo para a melhoria da eficiência operacional, da proteção dos ativos de informação e da continuidade dos serviços institucionais.

Ressalta-se que a Equipe de Planejamento da Contratação poderá revisar esta declaração caso surjam novos elementos relevantes durante a evolução dos estudos ou da instrução processual.

1.7.2. Justificativa:

A escolha da solução fundamenta-se na necessidade de aprimorar a capacidade institucional de prevenção, detecção e resposta a incidentes de segurança cibernética, diante do crescimento e da sofisticação das ameaças digitais que impactam ambientes corporativos e órgãos públicos.

A alternativa selecionada apresentou maior aderência aos requisitos técnicos e operacionais definidos no Estudo Técnico Preliminar, proporcionando maior nível de proteção aos ativos tecnológicos institucionais, especialmente aos endpoints e servidores que suportam os sistemas judiciais e demais serviços essenciais.

Adicionalmente, a solução escolhida apresenta melhor relação entre custo, eficiência operacional e capacidade de resposta a incidentes quando comparada à manutenção de soluções tradicionais baseadas

exclusivamente em antivírus, contribuindo para o fortalecimento da postura de segurança da informação e para a continuidade dos serviços institucionais.

2. SUSTENTAÇÃO DO CONTRATO

2.1. Adequação do Ambiente

Item	Descrição	SIM	NÃO
1	Necessidade de adequação de infraestrutura tecnológica?	X	
2	Necessidade de adequação de infraestrutura elétrica?		X
3	Necessidade de adequação de logística de implantação?	X	
4	Necessidade de adequação de espaço físico?		X
5	Necessidade de adequação de mobiliário?		X
6	Haverá impacto ambiental?		X

2.2. Recursos Materiais e Humanos

Necessidade de outras contratações: Não há necessidade de realizar outras contratações paralelas para a execução da contratação principal. O objeto configura um sistema único e integrado de proteção de endpoint e proteção contra ataques avançados, que deve ser fornecido pelo mesmo fabricante e executado por profissionais especializados na solução. A própria contratante já disponibilizará a infraestrutura de hardware e software necessária e existente em seu ambiente (como ambiente virtualizado, sistema operacional e banco de dados) para a instalação e configuração da solução. As ferramentas e equipamentos necessários à manutenção do sistema serão de responsabilidade exclusiva da contratada.

Recursos Humanos e Terceirização: O suporte técnico proativo, corretivo e de resposta a incidentes deverá ser prestado por profissionais terceirizados da CONTRATADA que sejam obrigatoriamente certificados pelo fabricante da solução, em nível compatível com a prestação do serviço.

Treinamentos e Capacitação: A contratação já engloba o "Serviço de capacitação e repasse de conhecimento". A CONTRATADA deverá ministrar treinamento na modalidade presencial (ou virtual, conforme definição do edital) de no mínimo 40 (quarenta) horas para a equipe técnica definida pelo TJAC. Este treinamento abrangerá aspectos teóricos e práticos, incluindo instalação, uso, configuração, análise de relatórios e resposta a incidentes, garantindo que os servidores compreendam e aproveitem plenamente as funcionalidades da solução.

Fiscalização e Gestão Contratual: A fiscalização do contrato deverá ser efetuada por um Fiscal de Contrato designado, que deve ser obrigatoriamente um servidor efetivo do PJAC e possuir a experiência necessária para a gestão e o acompanhamento de contratos de serviços de TIC.

2.3. Continuidade do Fornecimento

Natureza da necessidade: A necessidade do objeto é permanente, tratando-se de um serviço continuado devido à sua natureza essencial, o que significa que não pode haver interrupção ou descontinuidade.

Efeitos da descontinuidade: Qualquer interrupção no serviço de segurança teria um impacto imediato e grave no andamento das atividades do TJAC. A descontinuidade deixaria vulnerável o parque computacional de 2500 estações de trabalho e servidores, resultando em alto risco de impactos negativos como prejuízos financeiros, problemas operacionais, danos à imagem da Justiça Estadual, vazamento de dados pessoais (ferindo a LGPD) e sequestro de dados (ransomware).

Estratégias de Transição: Devido às características específicas do objeto (licenciamento de software e prestação de serviço de segurança contínua com garantia e suporte por 24 meses), o Termo de Referência deve estabelecer que não serão necessários procedimentos de transição e finalização do contrato. No entanto, para evitar o término da proteção, a Administração deve planejar a renovação contratual ou um novo certame tempestivamente, dentro do período de vigência.

Hipóteses de descontinuidade e ações (Matriz de Riscos): As hipóteses que podem motivar a interrupção contratual e suas respectivas ações e estratégias de mitigação estão mapeadas na Matriz de Alocação de Riscos, conforme aplicável ao TJAC:

1. Incapacidade de execução do objeto (Serviço executado em qualidade inferior ao exigido): Risco alocado à Contratada. A ação adotada pela Administração será a aplicação das sanções administrativas cabíveis.

2. Problemas de desempenho do sistema (lentidão ou falhas frequentes que afetem a usabilidade): Risco alocado à Contratada. A estratégia de mitigação envolve a realização de testes de desempenho abrangentes e a garantia de infraestrutura adequada de TI.

3. Ausência de recursos orçamentários e financeiros: Risco alocado ao Contratante (TJAC). A ação será prover os meios necessários para a viabilização dos recursos, evitando a suspensão dos serviços por falta de pagamento.

4. Caso fortuito ou força maior: Risco alocado ao Contratante (TJAC). A ação mitigadora será o reequilíbrio econômico-financeiro excepcional ou, em último caso, a resolução do contrato se o sinistro impedir a continuidade da execução

2.4. Transição Contratual e encerramento do contrato

Atividades técnicas para a transição/encerramento do contrato: Embora a natureza da solução (licenciamento de software de segurança em nuvem) minimize a necessidade de uma transição complexa, as seguintes atividades técnicas deverão ser rigorosamente cumpridas no encerramento do contrato:

a. Entrega de versões finais dos produtos alvos da contratação: A Contratada deverá disponibilizar a exportação de todos os logs de auditoria, históricos de incidentes de segurança, relatórios de vulnerabilidades e a documentação final das políticas e regras implementadas no ambiente do TJAC, em formatos de mercado (como CSV, PDF, XML).

b. Devolução de recursos materiais: A Contratada deverá devolver toda e qualquer informação confidencial gerada e/ou manipulada em decorrência do contrato (seja em meio físico, magnético ou eletrônico). Ferramentas e equipamentos de propriedade da contratada utilizados para a manutenção deverão ser retirados das dependências do TJAC.

c. Revogação de perfis de acesso: Imediatamente após o término do contrato, a equipe de TI do TJAC e a gestão do contrato deverão garantir a revogação de todos os perfis de acesso (credenciais de Active Directory, acessos VPN, acessos a servidores e bancos de dados) concedidos aos profissionais terceirizados da Contratada para prestação do suporte técnico.

2.5. Estratégia de Independência Tecnológica

Por se tratar de uma solução de mercado baseada em licenciamento, o TJAC não possuirá os direitos de propriedade intelectual sobre o código-fonte do software. No entanto, o TJAC reterá a propriedade integral e exclusiva sobre todos os dados, logs, informações sensíveis e arquitetura de regras/políticas geradas durante o uso da ferramenta.

A solução deve permitir, a qualquer momento e especialmente no encerramento do contrato, a exportação facilitada de painéis, políticas de segurança, configurações e históricos de detecção de ameaças. Isso garante que o TJAC possa migrar seu ambiente de proteção para outro fabricante no futuro sem perda do histórico de inteligência adquirido.

A independência da equipe do TJAC em relação à Contratada é assegurada pela execução obrigatória do treinamento especializado. Este repasse de conhecimento capacitará os servidores do Tribunal a instalarem, parametrizarem, monitorarem e atuarem na resposta a incidentes de forma autônoma, garantindo

que o Tribunal não fique operacionalmente dependente do fornecedor para a gestão diária da segurança cibernética.

3. ESTRATÉGIA PARA A CONTRATAÇÃO

3.1. Natureza do Objeto

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 endpoint, 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 exposto a vulnerabilidades e ataques.

O objeto envolve o fornecimento de uma solução de mercado (entregue na modalidade de serviço em nuvem / licenciamento). Sendo assim, os direitos de propriedade intelectual e autorais sobre o código-fonte da aplicação, os motores de detecção e o software em si são de titularidade exclusiva da empresa Contratada (ou do fabricante da solução). Essa exclusividade justifica-se por se tratar de uma solução comercial fechada (off-the-shelf). Em contrapartida, o TJAC reterá a propriedade integral e exclusiva sobre todos os dados, informações, bases de dados de auditoria, históricos de incidentes, logs e regras/políticas de segurança que forem gerados, parametrizados e documentados ao longo da vigência do contrato.

3.2. Parcelamento do Objeto e Adjudicação

Em observância à Lei nº 14.133/2021, o objeto não será parcelado em lotes independentes para múltiplos fornecedores. A solução será agrupada em um único grupo de itens.

Justificativa Técnica e Econômica: O objeto configura um sistema único e integrado de proteção (abrangendo e-mail, endpoint, rede e resposta a incidentes). Devido à natureza intrínseca e interdependente dessas funcionalidades, o parcelamento inviabilizaria a execução contratual, gerando baixo rendimento operacional e graves conflitos de execução. Não há vantagem técnica ou econômica para o TJAC em possuir diversos produtos diferentes de fabricantes distintos, sem continuidade e sem integração nativa, pois isso enfraqueceria o modelo de compliance e segurança cibernética.

Análise de Riscos do Agrupamento: O risco de inexecução satisfatória ao agrupar os itens é mitigado pela exigência de que todos os componentes sejam fornecidos por um mesmo fabricante e implementados por profissionais com certificação técnica específica. Por outro lado, o risco de parcelar a solução seria altíssimo, resultando em complexidade adicional para gerenciar múltiplos fornecedores, custos elevados de integração, incompatibilidade de tecnologias e lacunas na detecção correlacionada de ameaças avançadas.

3.2.1. Adjudicação do Objeto

O objeto será adjudicado pelo critério de Menor Preço Global (ou Menor Preço por Grupo), contemplando todos os itens, haja vista a natureza indivisível da solução.

Não será permitida a participação de empresas em consórcio. A vedação justifica-se pela natureza avançada e altamente especializada da solução de segurança. Permitir consórcios criaria desafios na coordenação técnica entre múltiplos parceiros, diluindo responsabilidades. É essencial para o TJAC que uma única entidade contratada seja inteiramente responsável por todas as fases (implantação, suporte e garantia).

É expressamente vedada a subcontratação, no todo ou em parte, do objeto. Por lidar com informações sensíveis e estratégicas da Justiça (dados de usuários, configurações, incidentes), a subcontratação introduziria riscos inaceitáveis à segurança da informação, aumentando o número de entidades com acesso aos dados. Além disso, a execução exige expertise técnica direta da contratada; a subcontratação causaria perda de controle sobre a qualidade do serviço, dificuldades na comunicação e obstáculos para apuração de responsabilidades em caso de falhas ou vazamentos.

3.3. Modalidade e Tipo de Licitação

A modalidade de licitação a ser adotada pelo TJAC será o Pregão, na sua forma Eletrônica. A escolha desta modalidade é obrigatória e justificada pelo fato de que a solução de segurança (proteção de e-mail, endpoint e redes) enquadra-se na categoria de bens e serviços comuns, por possuir padrões de desempenho e características gerais e específicas que são usualmente encontradas e consolidadas no mercado de TI.

O critério de julgamento (tipo de licitação) será o de Menor Preço por Grupo (Menor Preço Global), regido pela Lei Federal nº 14.133/2021

3.4. Vigência do contrato

O prazo de vigência do contrato a ser firmado pelo TJAC será de 24 (vinte e quatro) meses, contados a partir da data de sua assinatura. Por se tratar de um serviço continuado e de natureza essencial (cuja interrupção causaria impacto imediato às atividades do Tribunal).

É importante destacar que a vigência do instrumento contratual não se confunde com a vigência da garantia. Enquanto o contrato passa a vigorar a partir de sua assinatura, a garantia contratual e o suporte técnico (que também possuem prazo de 24 meses) começarão a ser contados apenas a partir do primeiro dia útil subsequente à data de emissão do Termo de Recebimento Definitivo da solução. A garantia não se limita ao término da vigência contratual original.

3.5. Equipe de Apoio à Contratação

Nome	Cargo	Matrícula	Setor
Elielcio Canedo da Silva	Subsecretário	7000710	SUCTI
Ângelo Máximo de Melo Silva	Chefe de Divisão	7002075	DICTI

3.6. Equipe de Gestão do Contrato

Nome	Cargo	Matrícula	Setor
Elson Correia de Oliveira Neto	Gestor Titular	7001778	SETIC

3.7. Equipe de Fiscalização do Contrato

Nome	Cargo	Matrícula	Setor
Elinara Bras Ferreira	Fiscal Titular	7002145	DISEG
Gerson Oliveira da Silva Junior	Fiscal Substituto	7002070	DISEG

4. ANÁLISE DE RISCOS

Em atenção ao artigo 18, inciso X, da Lei Federal nº 14.133/2021, que destaca a importância da gestão de riscos para o sucesso da licitação e execução contratual, bem como ao artigo 10 da Resolução CNJ nº 468/2022, que prevê ações de gerenciamento de riscos e a elaboração do mapa de gerenciamento, e que este deve ser juntado ao processo de contratação após a elaboração dos Estudos Técnicos Preliminares.

É importante mencionar que, conforme disposto no artigo 22 da Lei Federal nº 14.133/2021, o edital poderá contemplar matriz de alocação de riscos entre o contratante e a Contratada, hipótese em que o cálculo do valor

estimado da contratação poderá considerar taxa de risco compatível com o objeto da licitação e com os riscos atribuídos à Contratada, de acordo com metodologia predefinida pelo ente federativo.

De acordo com o art. 22, § 3º da Lei Federal nº 14.133/2021, para contratações de grande vulto, é obrigatório que o edital inclua o Mapa de Gerenciamento de Riscos, que aloca os riscos entre o contratante e a Contratada. Para contratações de menor vulto, a exigência desse artefato fica a critério do órgão, que deve definir o valor estimado para a não exigência do mesmo.

Dessa forma, é ressaltada a importância da elaboração do mapa de gerenciamento de risco, sua criação dependerá de critérios e valores mínimo definidos por normativo específico de cada órgão.

O tratamento dos riscos deve ocorrer ao longo de todo o processo de contratação e de gestão do contrato. Entretanto, o Mapa de Gerenciamento de Riscos deve ser atualizado, no mínimo:

- ao final da elaboração dos estudos técnicos preliminares;
- ao final da elaboração do termo de referência; e
- após eventos relevantes.

Neste tópico, são assinalados os principais riscos detectados envolvidos na contratação e na gestão do contrato.

4.1. Riscos Mapeados

Risco 1	**Risco:**	**Falha na Integração/Implantação:** A solução XDR não se integrar adequadamente com sistemas legados ou não ser totalmente implantada.	
	Probab.:	Média	
	Impacto:	Alto	
	Dano 1:	Lacunas na visibilidade e proteção, inoperância da solução, atraso no cronograma e retrabalho.	
	Tratamento:	Planejamento detalhado da integração, testes em ambiente de homologação, comunicação e coordenação constantes entre PJAC e fornecedor.	
	Id	**Ação Preventiva**	**Responsável**
	1	Elaborar plano de integração e implantação com fases claras e validação em cada etapa.	PJAC - Equipe SUSEG
	2	Realizar testes de ponta a ponta em ambiente controlado (piloto/homologação).	PJAC - Equipe SUSEG, Fornecedor XDR
	3	Designar equipe técnica interna dedicada para acompanhamento próximo do processo.	PJAC - Equipe TI/Infraestrutura
	Id	**Ação Contingência**	**Responsável**
	1	Acionar equipe de consultoria externa especializada em integrações complexas de segurança para análise e suporte.	PJAC - Gestor Contrato, Equipe SUSEG
	2	Reverter para a solução de segurança anterior (se viável) na parcela dos ativos não protegidos, mantendo a operação da solução XDR onde foi bem-sucedida.	PJAC - Gestor Contrato, Equipe SUSEG

Risco 2	**Risco:**	**Impacto no Desempenho:** Agentes XDR causarem impacto significativo no desempenho de Endpoints e Servidores.	
	Probab.:	Média	
	Impacto:	Alto	
	Dano 2:	Lentidão nas máquinas, insatisfação dos usuários, interrupção de atividades, resistência à adoção da solução.	
	Tratamento:	Testes de desempenho rigorosos em ambiente piloto, otimização das configurações do agente XDR.	
	Id	**Ação Preventiva**	**Responsável**
	1	Executar testes de desempenho exaustivos em grupos pilotos antes do rollout massivo.	PJAC - Equipe TI/Infraestrutura
	2	Otimizar as configurações de varredura e detecção para menor consumo de recursos.	Fornecedor XDR, PJAC - Equipe SUSEG
	3	Definir requisitos mínimos de hardware nos termos do contrato e na documentação técnica.	PJAC - Equipe TI/Infraestrutura
	Id	**Ação Contingência**	**Responsável**
	1	Desabilitar temporariamente módulos específicos do agente XDR (ex: monitoramento comportamental) que estejam causando o impacto, com notificação e acompanhamento do fornecedor.	PJAC - Equipe TI/Infraestrutura, Equipe SUSEG
	2	Reduzir o escopo da implantação para um número menor de ativos críticos, ou retornar à solução anterior nos ativos afetados, enquanto se busca uma solução com o fornecedor.	PJAC - Gestor Contrato, Equipe TI/Infraestrutura

Risco 3	**Risco:**	**Dependência Tecnológica/Conhecimento:** Insuficiente transferência de conhecimento para a equipe interna do PJAC.	
	Probab.:	Média	
	Impacto:	Alto	
	Dano 3:	Aumento de custos com suporte externo, dificuldade na operação e otimização, impedimento para futuras transições.	
	Tratamento:	Plano de capacitação intensivo, envolvimento ativo da equipe interna na implantação e operação.	
	Id	**Ação Preventiva**	**Responsável**
	1	Exigir treinamento hands-on e certificações formais para a equipe do PJAC.	do PJAC.PJAC - Gestor Contrato
	2	Incluir cláusulas de co-implementação e mentoria da equipe interna pelo fornecedor.	do PJAC.PJAC - Gestor Contrato
	3	Criar e manter uma base de conhecimento interna para a solução XDR.	PJAC - Equipe SUSEG
	Id	**Ação Contingência**	**Responsável**
	1	Contratar consultoria pontual para treinamento in loco e hands-on intensivo, focado nas lacunas de conhecimento identificadas.	PJAC - Gestor Contrato, Gestor de TI/SUSEG
	2	Realocar recursos humanos internos, dedicando-os exclusivamente à capacitação e operação da XDR por um período determinado.	PJAC - Gestor de TI/SUSEG

Risco 4	**Risco:**	**Sobrecarga de Alertas:** Grande volume de falsos positivos ou alertas irrelevantes.	
	Probab.:	Alta	
	Impacto:	Médio	
	Dano 4:	Fadiga de alertas, perda de incidentes reais no meio do volume, ineficiência da equipe de segurança.	
	Tratamento:	Refinamento contínuo das políticas de detecção, **tuning** da solução e capacitação da equipe em **threat hunting**.	
	Id	**Ação Preventiva**	**Responsável**
	1	Implementar processo de **tuning** e calibração das regras de detecção pós-implantação.	PJAC - Equipe SUSEG
	2	Capacitar a equipe em análise de alertas, investigação eficiente e **threat hunting**	PJAC - Equipe SUSEG
	3	Estabelecer processos de triagem e priorização de alertas para otimizar o fluxo de trabalho.	PJAC - Equipe SUSEG
	Id	**Ação Contingência**	**Responsável**
	1	Priorizar e focar a análise apenas em alertas de alta e média severidade, suspendendo temporariamente a investigação de alertas de baixa severidade.	PJAC - Equipe SUSEG
	2	Acionar o fornecedor para *tuning* emergencial e suporte *on-site* na triagem e otimização das políticas de detecção, se a equipe interna não conseguir resolver.	PJAC - Gestor Contrato, Equipe SUSEG

5. APROVAÇÃO E ASSINATURA

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, aprovam o Estudo Técnico Preliminar e atestam sua conformidade às disposições da Resolução CNJ nº 468/2022.

6. CIÊNCIA DA INSTÂNCIA DELIBERATIVA DE TIC

Confirmo o recebimento do Estudo Técnico Preliminar, no qual tomo ciência de forma integral de seu conteúdo. A partir deste momento, segue para prosseguimento às providências cabíveis visando garantir o encaminhamento do ETP para a instância competente do órgão.

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

PODER JUDICIÁRIO
DO ESTADO DO ACRE

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

Elson Correia de Oliveira Neto
Secretário de Tecnologia da Informação e Comunicação
Autoridade Superior

Allexandra Macedo de Souza Oliveira
Chefe da Divisão de Contratações de TIC
Integrante Administrativo - Portaria nº 3847/2025/TJAC

Documento assinado eletronicamente por **AMILAR SALES ALVES**, **Gerente de Segurança da Informação** em 24/04/2026 às 13:48:37.

Documento assinado eletronicamente por **ELSON CORREIA DE OLIVEIRA NETO**, **Secretário(a)** em 24/04/2026 às 13:52:11.

Documento assinado eletronicamente por **ALLEXANDRA MACEDO DE SOUZA OLIVEIRA**, **Chefe de Divisão** em 27/04/2026 às 11:22:58.

Documento assinado eletronicamente por **ANGELO MAXIMO DE MELO SILVA**, em 27/04/2026 às 10:56:34.

Documento assinado eletronicamente por **ELIELCIO CANEDO DA SILVA**, **Técnico Judiciário** em 27/04/2026 às 10:50:06.